CISCO Connect

Navigating the Path to Zero Trust

Strategies for Migrating to ZTNA

Luke Hebditch
Solutions Engineer, SSE, EMEA
lhebditc@cisco.com

Zero trust isn't a product, it's an approach

Principles

Strategy

Architecture

Capabilities

Technologies

Features

cisco

Zero Trust principles

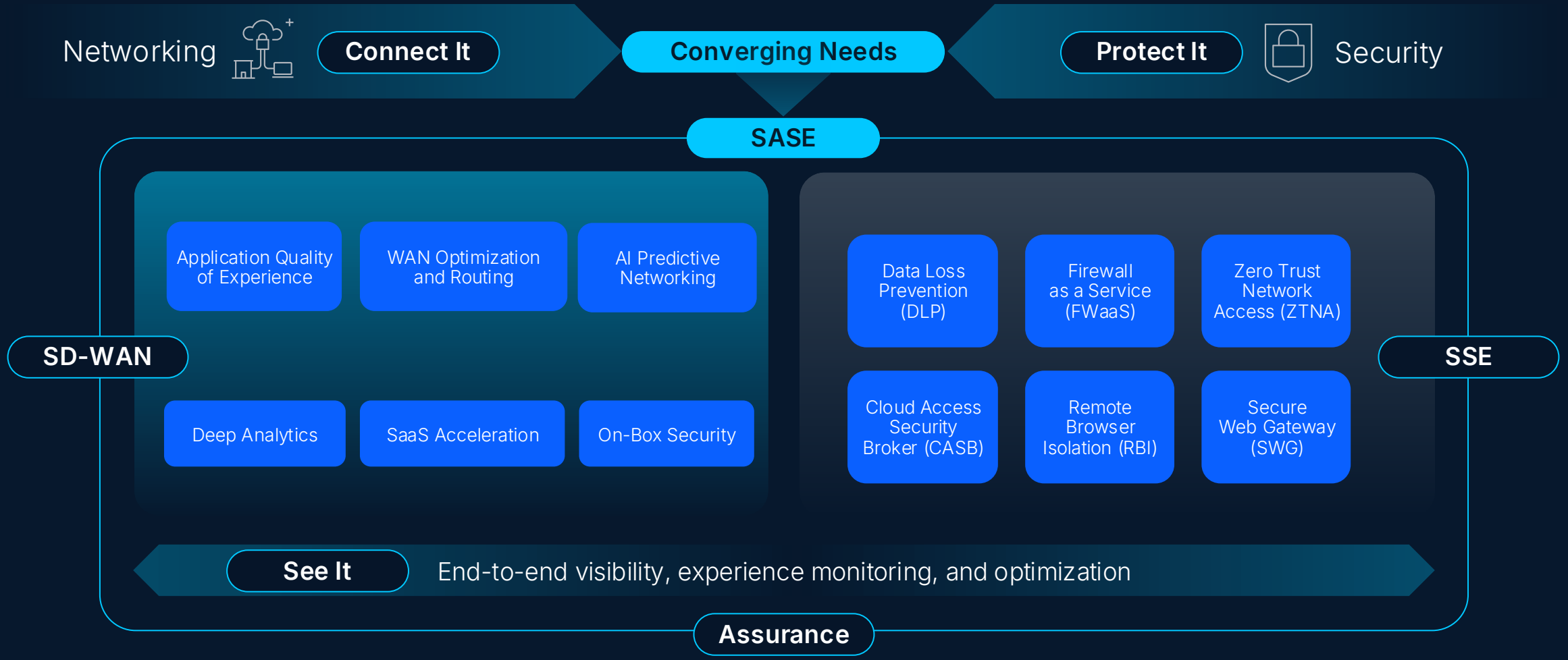
1. Never assume trust
2. Always verify
3. Enforce least privilege

Zero Trust success factors

1. Respect user privacy and user experience
2. Adjust policy to risk
3. Consistent experience across environments

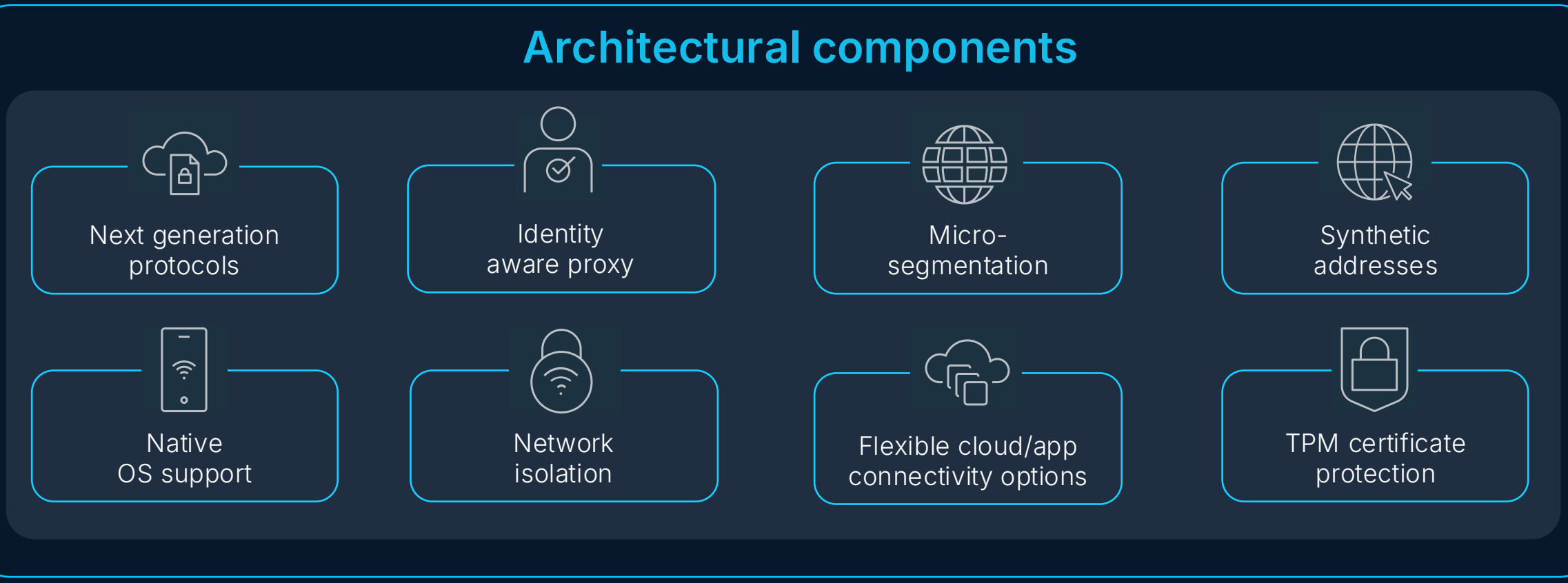
Secure Access Service Edge (SASE)

Single vendor SASE from Cisco helps you see it all, protect it all, and perform everywhere.



Modern Zero Trust Access Design (ZTNA)

Architectural components



ZTA for the ultimate in secure private access

Least privileged access

Efficient and secure access to all private apps

- Groundbreaking security
- Incredibly easy to use
- Faster than VPN

- Granular user driven access control protects resources
- Frictionless user experience boosts productivity
- Hardware protected keys to strongly authenticate users
- Hide resources to prevent attacker reconnaissance
- Unified dashboard enables operational simplicity
- Optimized latency/throughput for a superior user experience

ZTA: Next Generation Zero Trust Access

Migration approaches & considerations

Key questions to consider as part of defining an ZTNA project

- What is in scope? Private access ONLY or full SSE (incl internet access)? Zero trust for users only, or a wider scope?
- What is the state of the identity stack?
- Do we understand the applications in use in the environment and by whom?
- Is there a current SD-WAN deployment or plans to do so?
- What does our current private access setup look like? Single VPN platform, multiple platforms, policy/access controls
- Do the applications support ZTNA?

Application connectivity types to consider

1

Client to Server

Most applications

ZTNA
support this

2

Server to Client

Some legacy applications
Connectivity being established server-side to the client

ZTNA does NOT support this

3

Client to Client

Client to Client connectivity, such as two remote devices

ZTNA does NOT support this

How do you handle these 2 use cases?

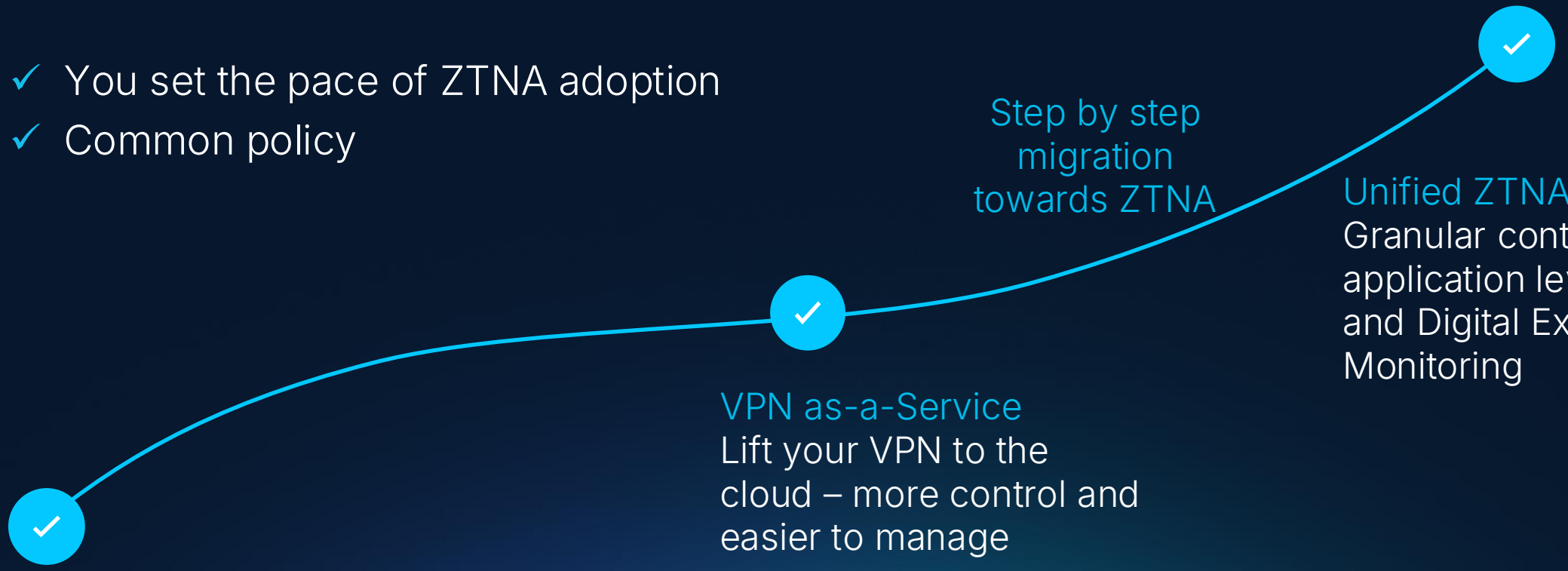
cisco

How to handle these use cases

- Decommission legacy applications
- Application/tool migration
- Split strategy
  - VPNaaS utilised alongside ZTNA

Easy migration to Zero Trust Access

- ✓ You set the pace of ZTNA adoption
- ✓ Common policy



Traditional VPN
Network level access
Typically on premise

VPN as-a-Service
Lift your VPN to the cloud – more control and easier to manage

Step by step migration towards ZTNA

Unified ZTNA
Granular controls at the application level + VPNaaS and Digital Experience Monitoring

Project considerations

Phased deployment

- Start small
- Platform validation
- UAT testing
- Deployment ring approach

Testing different user personas

- Include users from as many parts of the business as possible early to ensure different applications are tested

Collating feedback

- Ensure there is a clear process to enable end users to easily provide feedback
- Often little issues are not shared by users

Cisco Secure Access

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 (ZTA)
- Firewall as a Service (FWaaS) and IPS

Cisco delivers the core and more in a single subscription...

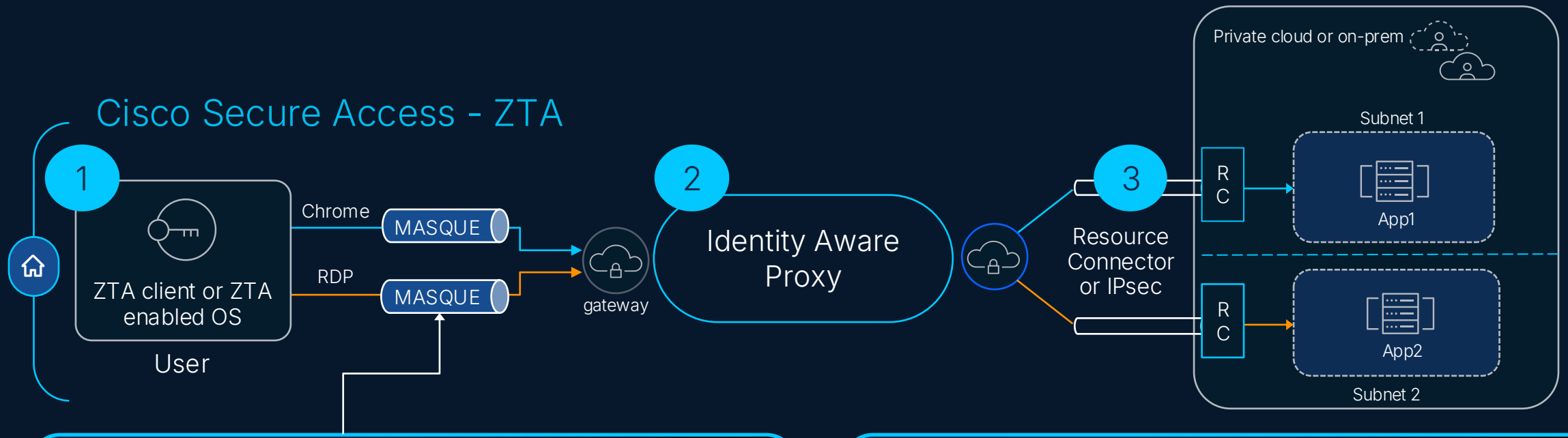
- DNS Security
- Multimode DLP
- Advanced Malware protection
- Sandbox
- Talos Threat Intelligence
- VPN as a Service
- Digital Experience Monitoring
- Remote Browser Isolation

Add-on solutions

- SD-WAN
- XDR
- DUO MFA/ SSO
- SSPM

How do we do it? MASQUE & QUIC Proxying!

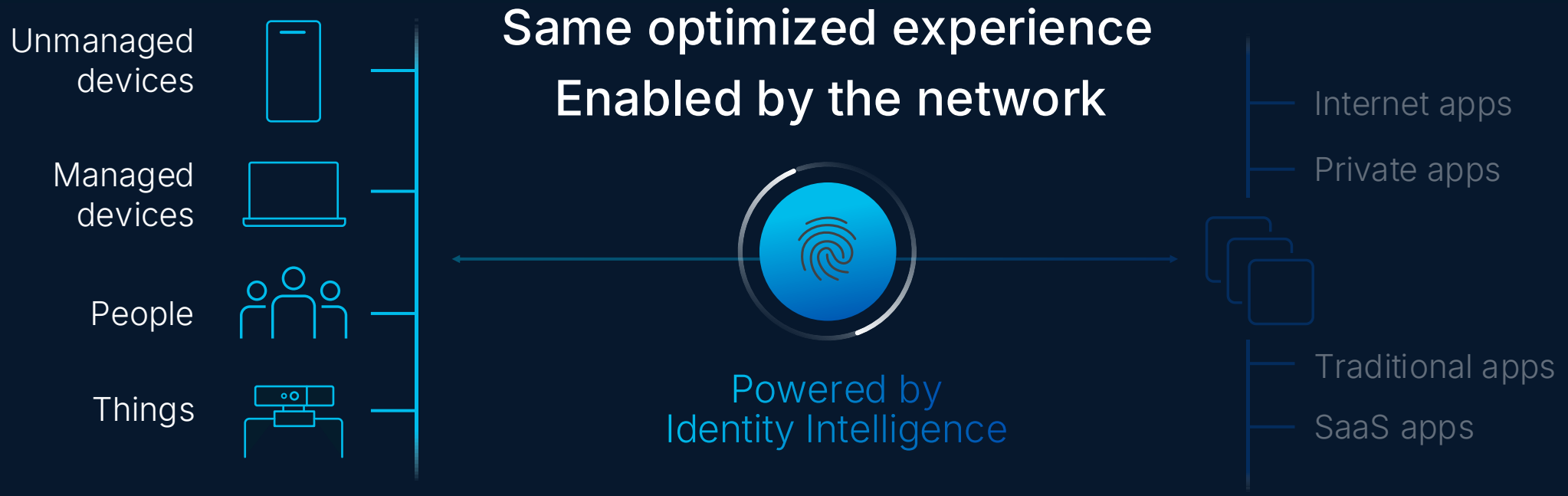
Seamless and Secure Access for all users



- 'No click' seamless access
- Advanced protocols reduce latency, improve resiliency and speed content delivery
- Credential Aliasing using ACME Certificates

- Full separation between user's network and the enterprise network
- Fast deployment with no firewall setting changes

Universal ZTNA from Cisco



Remote

Remote | Campus | Branch | Airplane | Oil rig | Stadium | Field | • • •

Cisco's Universal ZTNA

Secure SD-WAN + Security Service Edge + Trusted Identity Edge

SINGLE VENDOR SASE

End-to-end Assurance with ThousandEyes

Security Cloud Control

Cisco’s Unified SASE Management

Secure SD-WAN
Cisco SD-WAN

+

Secure Services Edge
Cisco Secure Access

+

Identity First
DUO + Identity Intelligence

Streamlined Management

One platform to manage SASE operations

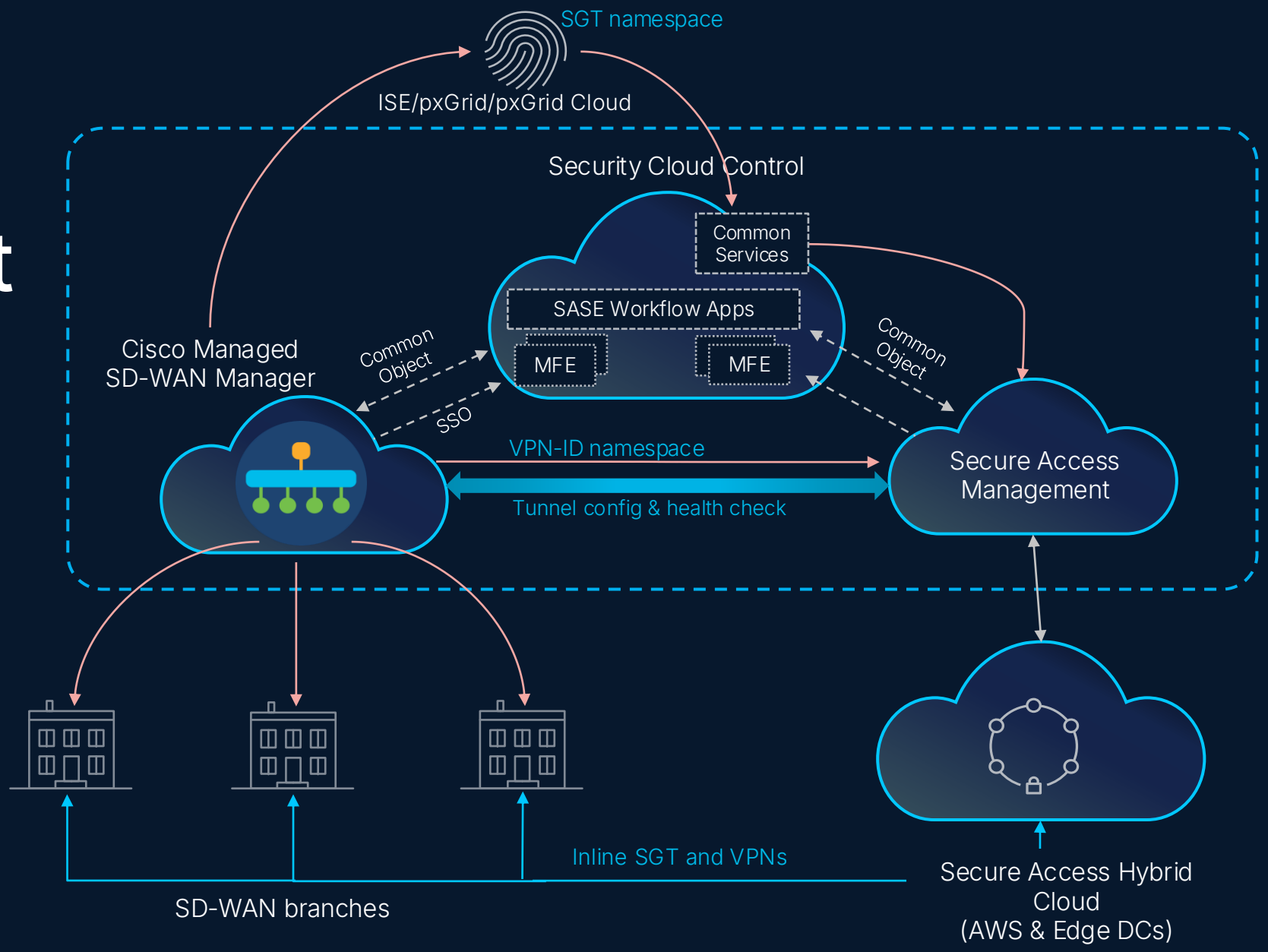
Consistent, Advanced Security

Centralized policies, enforced uniformly

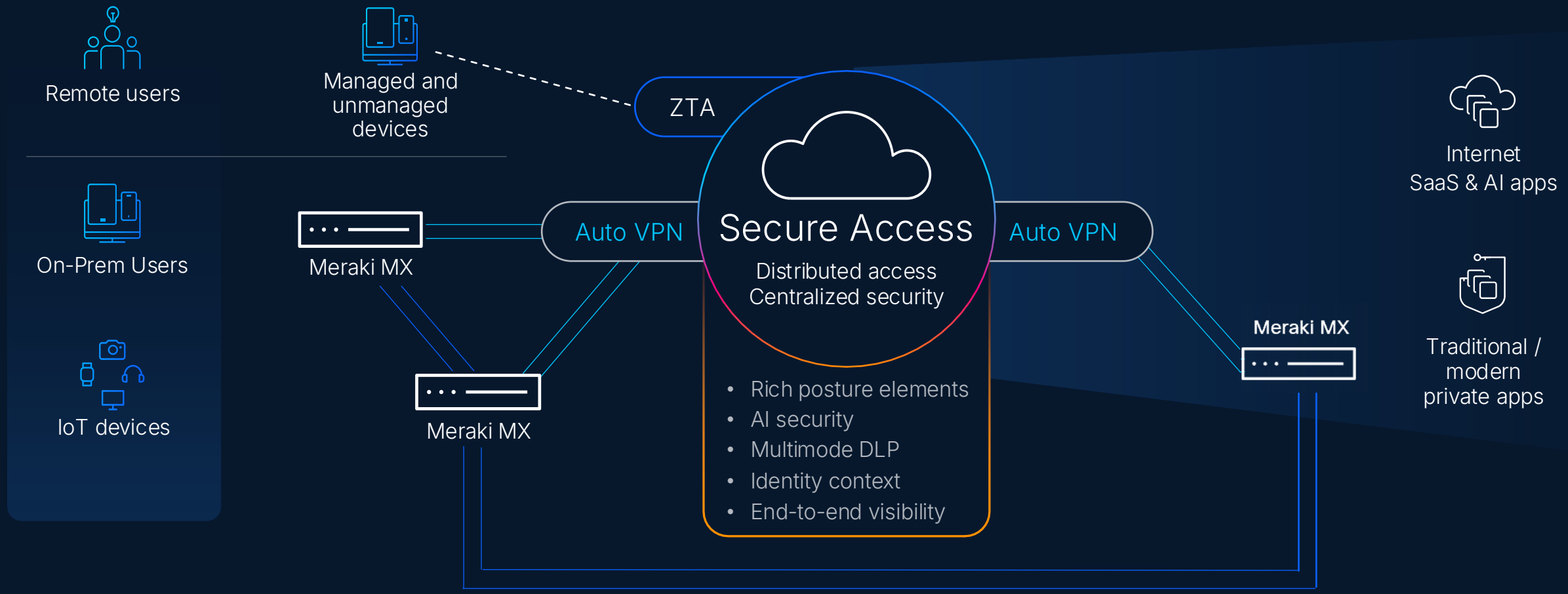
End-to-End Visibility

AI-powered insights across users, apps, devices

Cisco SASE with Catalyst



Cisco SASE with Meraki




CISCO