SASE, what is it?

BCS ISSG Early Careers Webinar

Luke Hebditch

- Technical Solutions Specialist, Cloud Security EMEAR, Cisco

- BCS ISSG Committee Member
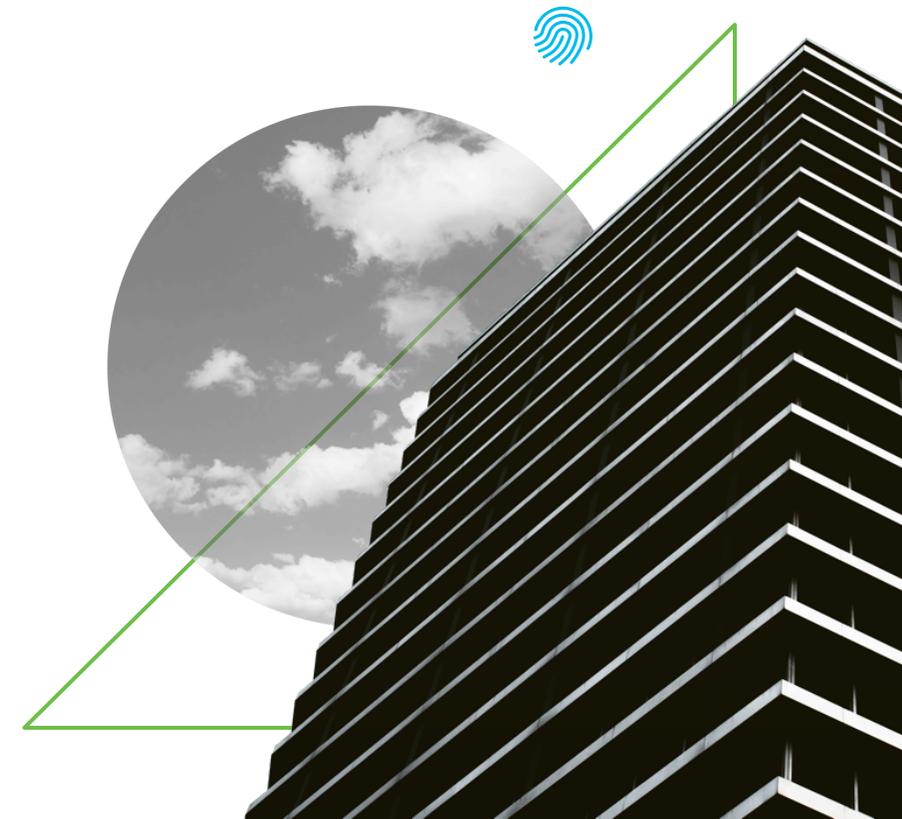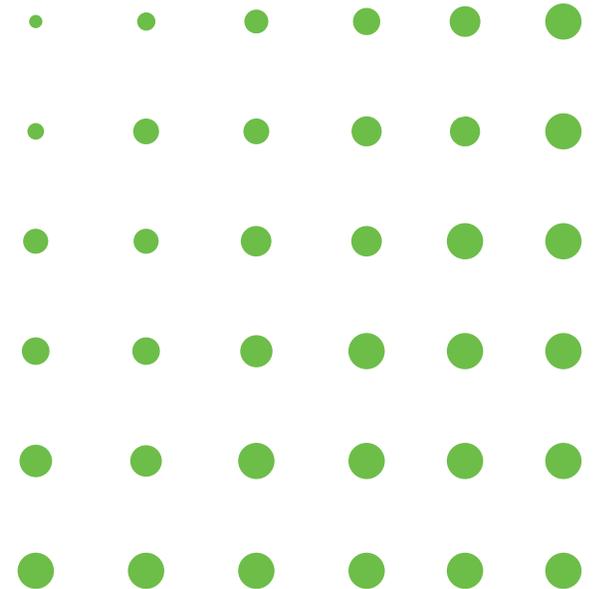
Thursday 1st April 2021

Agenda

- Who am I? My journey to today

- SASE, another buzzword?
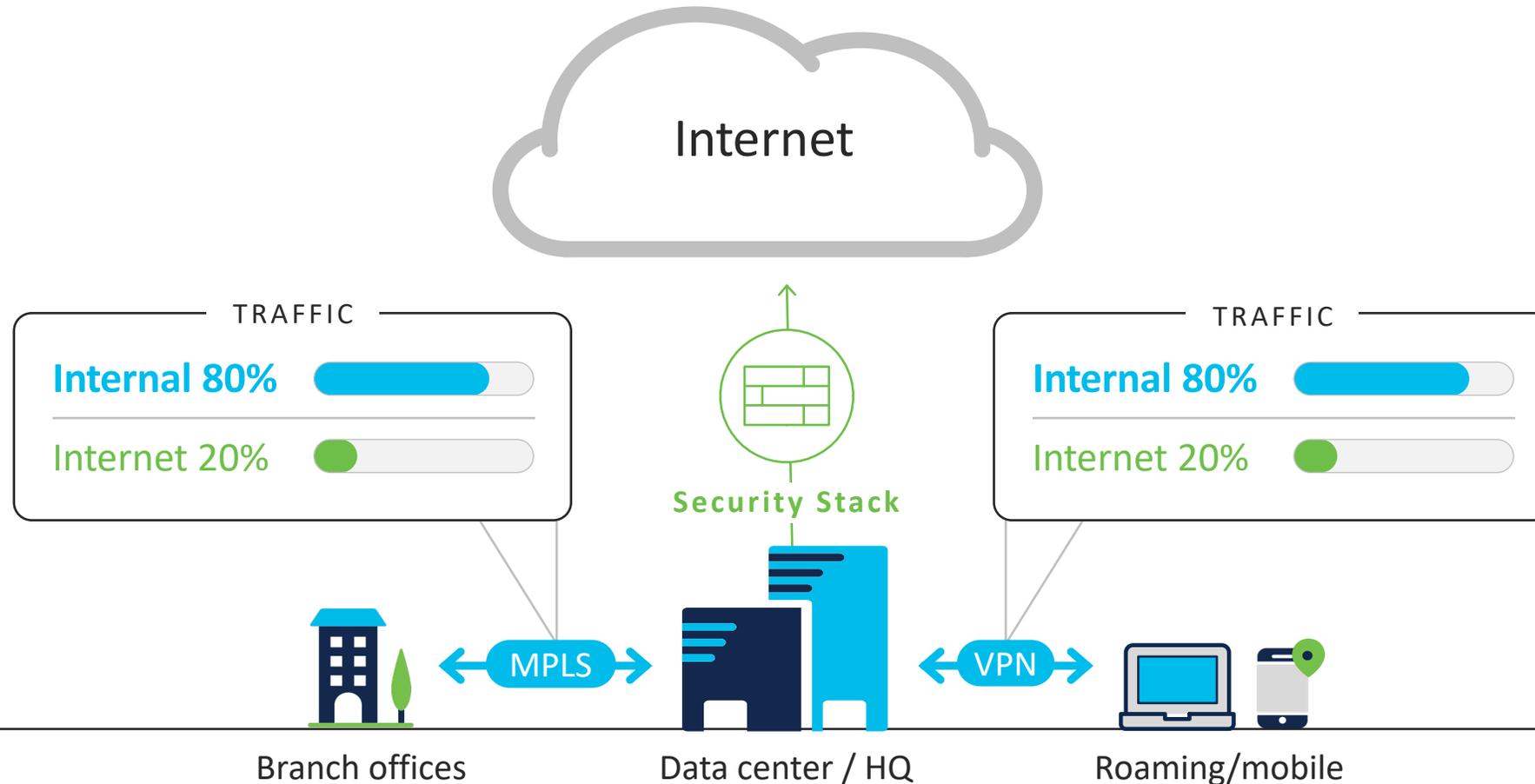
- Q&A

Luke Hebditch

- Technical Solutions Specialist, Cloud Security

- Cisco CCNP Certified in both Security and Enterprise

- Joined Cisco in 2016 via Degree Apprenticeship programme

- Graduated with a 1st – BSc Digital and Technology Solutions: December 2019

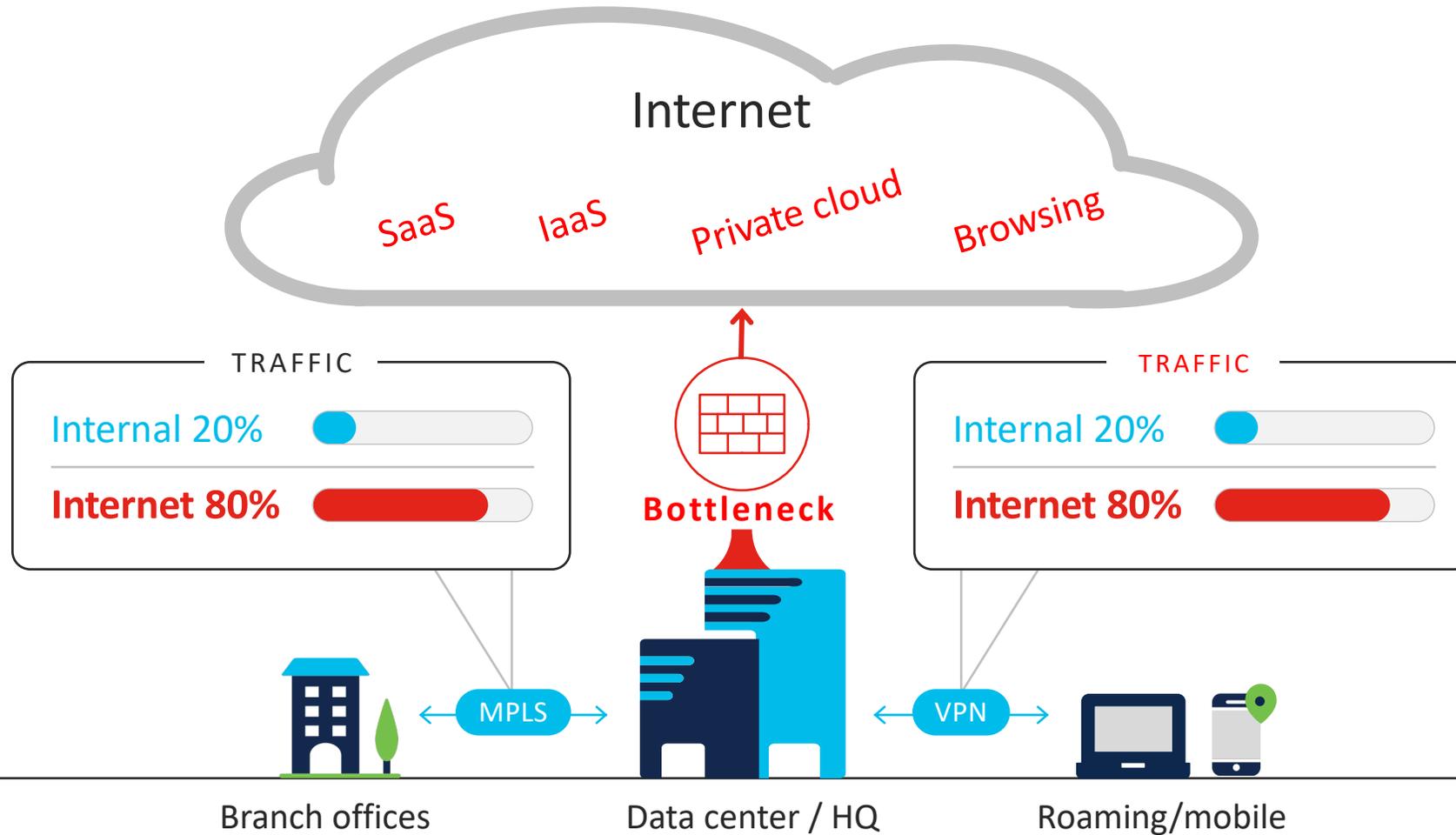# SASE, another buzzword?

Historic traffic flows led to the age of the single, on-premise security stack

Internet

TRAFFIC

Internal 80%

Internet 20%

Security Stack

TRAFFIC

Internal 80%

Internet 20%

MPLS

VPN

Branch offices

Data center / HQ

Roaming/mobile

Changes in the types of traffic, origins, and destinations have inverted the traffic model

Internet

SaaS   IaaS   Private cloud   Browsing

TRAFFIC
Internal 20%
Internet 80%

Bottleneck

TRAFFIC
Internal 20%
Internet 80%

MPLS

VPN
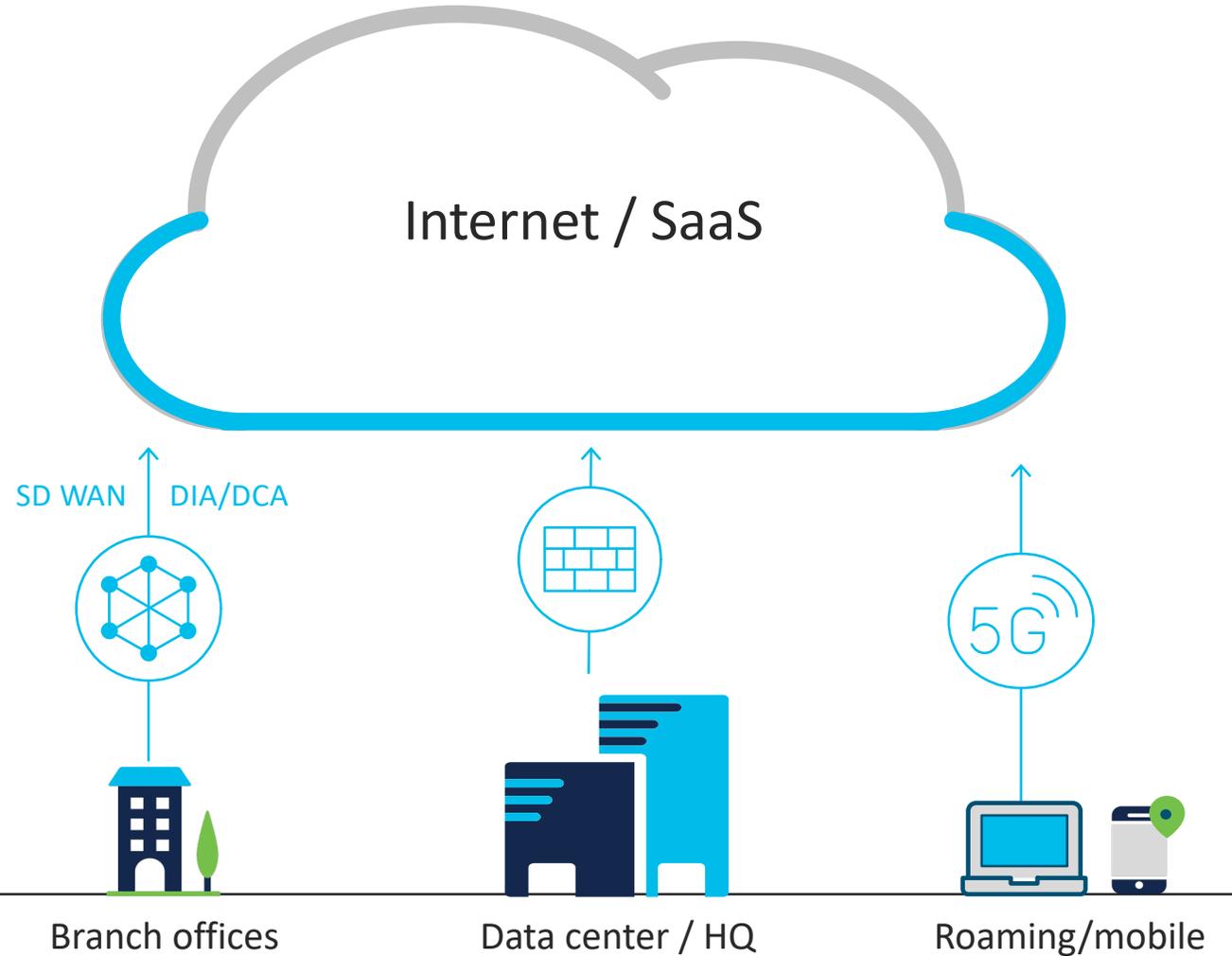
Branch offices

Data center / HQ

Roaming/mobile

Problems:

- Costs

- Performance

- # Tools/vendors
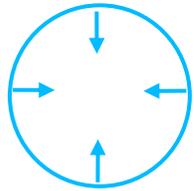
- Integrations

- Maintenance

A more modern "direct internet access" approach

Network:
Decentralized

Security:
Protect traffic from multiple locations at the cloud edge

Internet / SaaS

SD WAN | DIA/DCA

5G

Branch offices

Data center / HQ

Roaming/mobile

The nature of the network has changed

We are here

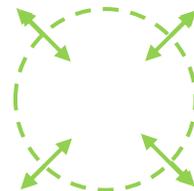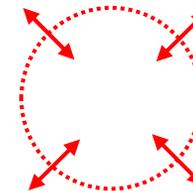| Firewall	Net	Extranet	Access	Intelligence
Keep data **within** the firewall	Manage data **inside** and **outside** the firewall	Manage data **through** the firewall	Manage data through **IDM** and **access control**	Dynamic content **data-centric** & **person-centric**
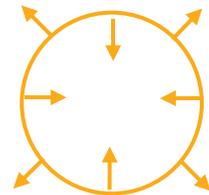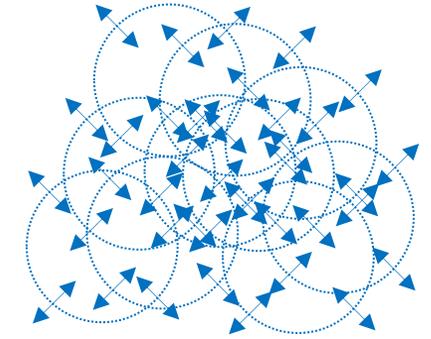
The Journey to Integrated Business-Security

Automated Threat Containment (XDR) / Zero Trust

Automate workflows with Integration / SOAR

Compliance & Posture

Unify Visibility

Centralised Logging UEBA/SIEM

Incident Response

Control Zones & Segmentation

NAC
Workloads

Expand Control

Guest
BYOD

Visibility & the basics

Patching
MFA/IAM
DNS
EDR
Monitoring

Fortify Perimeter

NGFW/IPS
WAF/DDoS
VPN
Email

System/network-centric security

Process-centric security

Improving security culture

Process/data-centric security: secure the workflow

Secure communications for email: CEO sending email to shareholder

CEO — Client-Based Security — Identity — Posture Assessment — Firewall — Intrusion Prevention — Flow Analytics — Threat Intelligence — Anti-Malware — Tagging — Application Visibility Control — Email Security — Server-Based Security — Shareholder

Secure applications for employees: Employee working remotely

Employee — Multi-factor Authentication — Identity — Posture Assessment — Firewall — Intrusion Prevention — Flow Analytics — Threat Intelligence — Anti-Malware — Tagging — Application Visibility Control — Web Application Firewall — Application-Based Security — Application

Secure web access for employees: Employee researching product information

Employee — Endpoint — Network — Application — Website

Secure communications for collaboration: Subject matter expert consultation

Expert — Endpoint — Network — Endpoint — Colleague

The typical first step to address these issues is to combine cloud-delivered security services

93%

of orgs agree that moving security to the cloud has increased efficiency
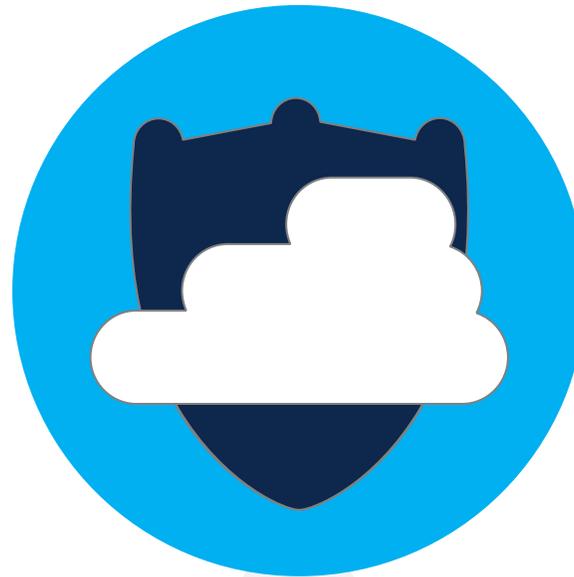
76%

of orgs are looking for multi-function cloud security services

DNS security

Secure web gateway

Firewall

Cloud Access Security Broker
CASB

Cloud and Network Evolution

Networks continue to decentralize

Applications and data are going to the cloud

Security and networking functions are converging

80%
of orgs are shifting to direct internet access (DIA)

76%
of orgs use SD-WAN extensively or selectively

42%
of branch office security deployments take over a month

68%
of branch offices and roaming users were the source of compromise in recent attacks

Next, reduce complexity and improve performance by unifying networking, security and identity
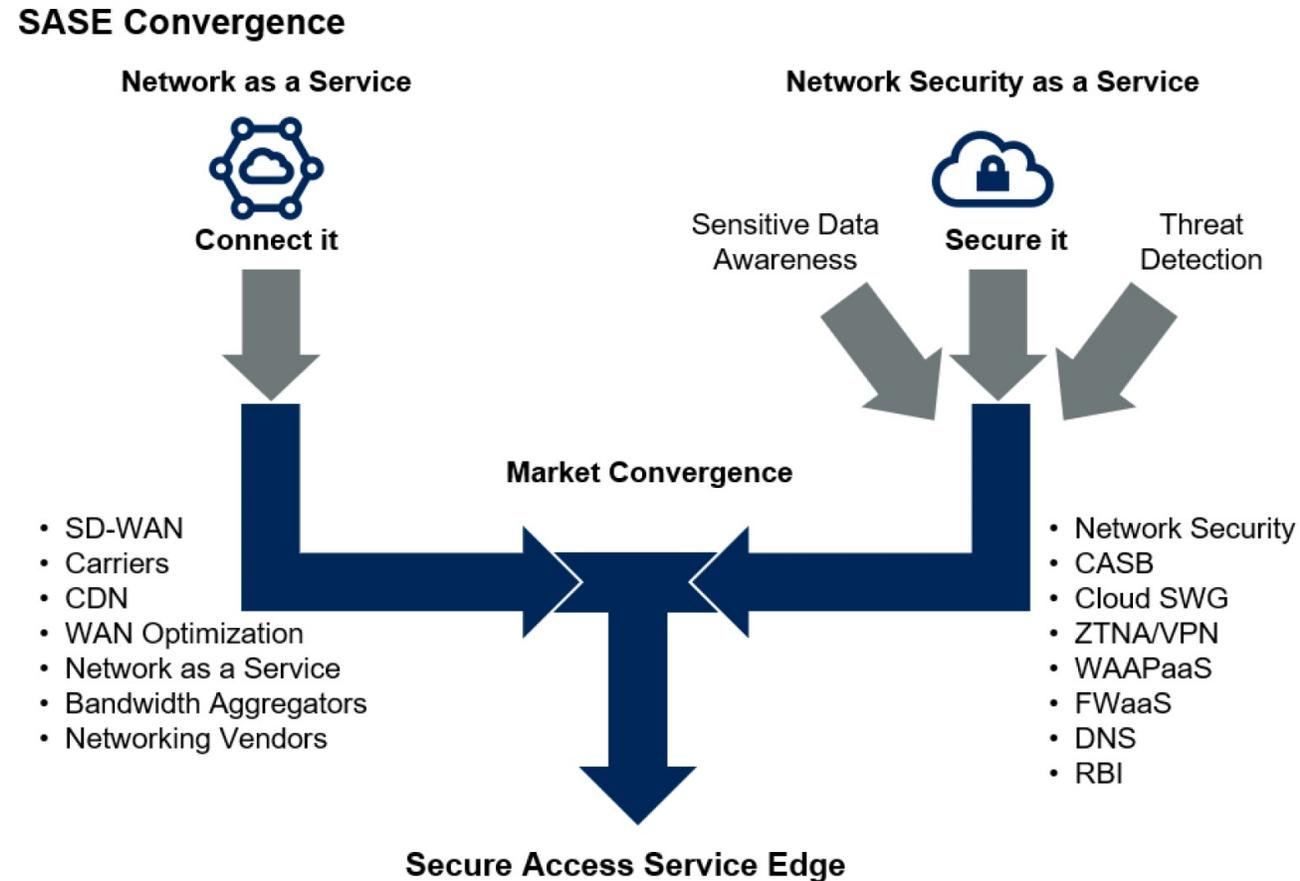
There are many names for this multi-function approach…

Gartner®

Secure Access Service Edge (SASE)

Convergence of networking & security services including SWG, CASB, DNS protection, firewall-as-a-service, SD-WAN, and zero trust network access

…but full agreement on the move to cloud-native aggregation

SASE Architecture Model Fundamentals (Gartner)

SASE Convergence

Network as a Service

Connect it

Network Security as a Service

Sensitive Data Awareness

Secure it

Threat Detection

Market Convergence

- SD-WAN
- Carriers
- CDN
- WAN Optimization
- Network as a Service
- Bandwidth Aggregators
- Networking Vendors

- Network Security
- CASB
- Cloud SWG
- ZTNA/VPN
- WAAPaaS
- FWaaS
- DNS
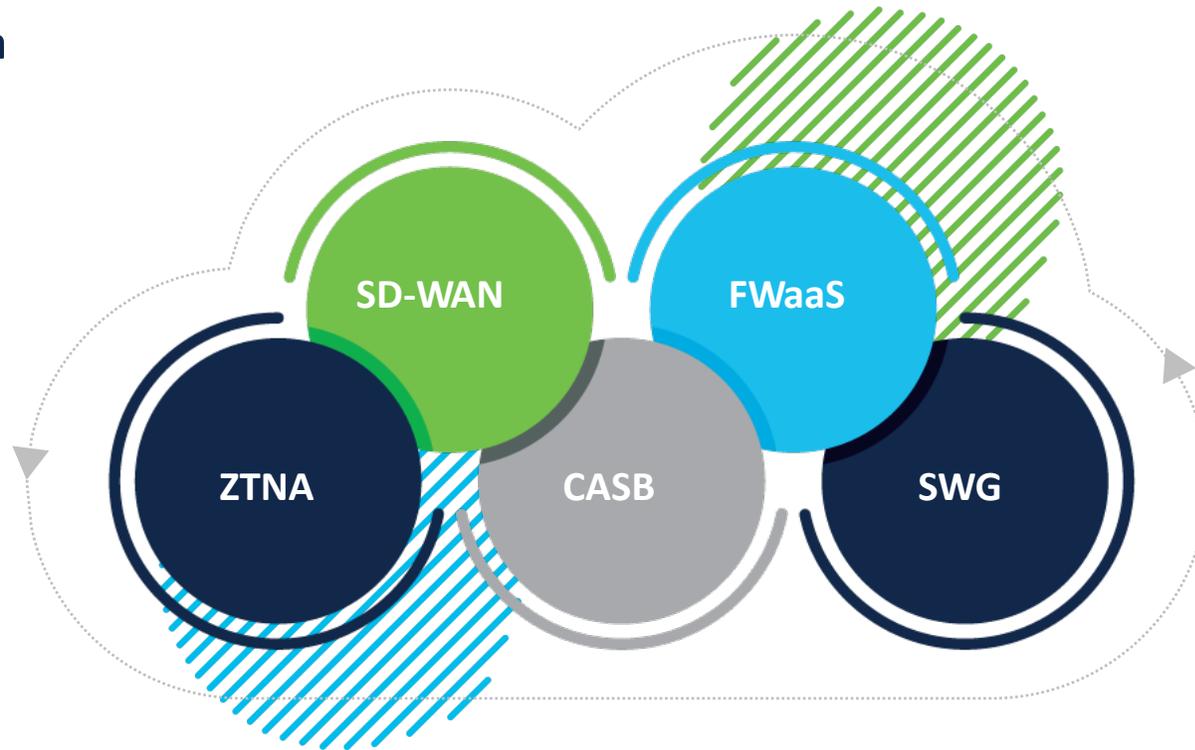- RBI

Secure Access Service Edge

CDN: content delivery network; RBI: remote browser isolation; WAAPaaS: web application and API protection as a service.
Source: Gartner
ID: 441737

Realizing SASE Architecture is a Journey

Consolidation through a single vendor

Effective security and threat protection

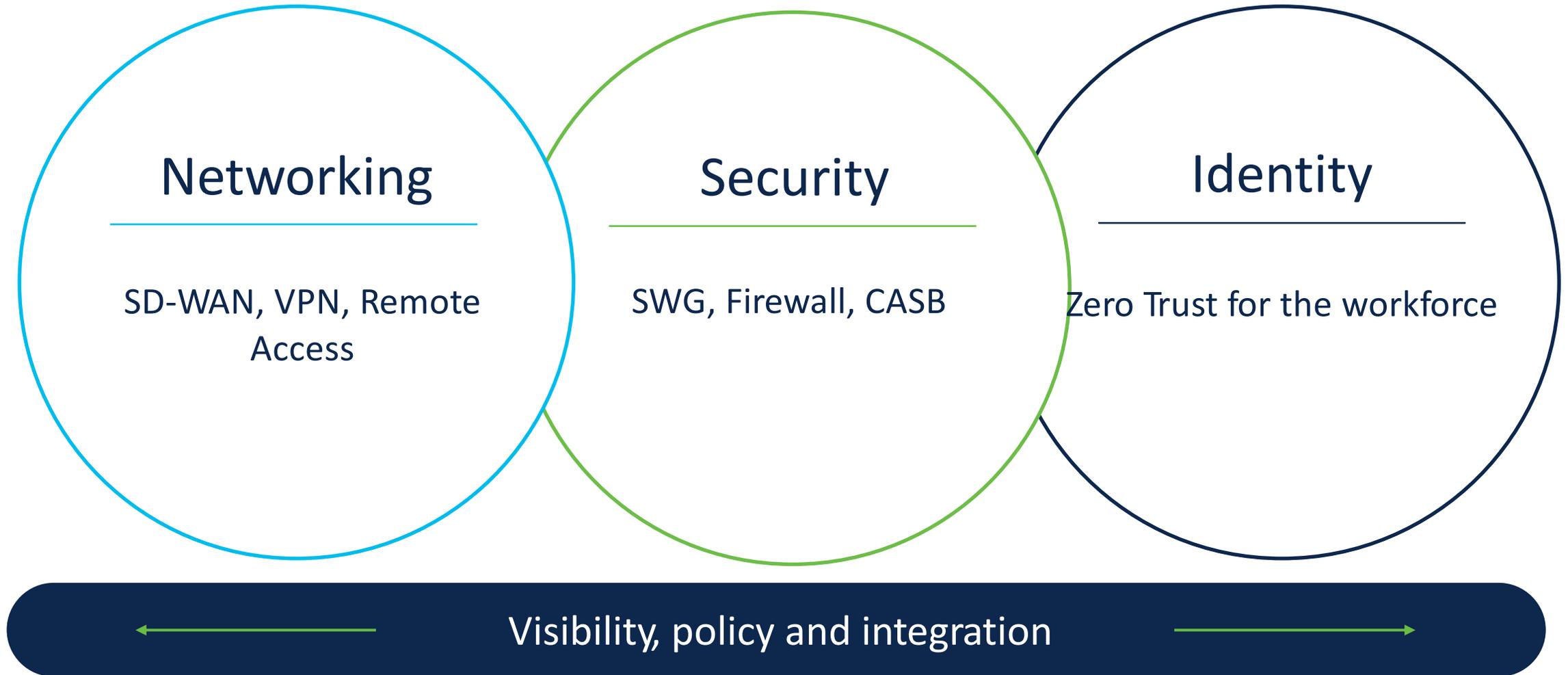**Global presence and peering relationships**

Support for all devices and agents

Microservices based architecture

Flexible deployment and management

SD-WAN

FWaaS

ZTNA

CASB

SWG

SASE includes more than security

Networking

SD-WAN, VPN, Remote Access

Security

SWG, Firewall, CASB

Identity

Zero Trust for the workforce

Visibility, policy and integration

Thank you