How to SASE, ZTNA and SD-WAN?

Patrick Commers – Fortinet Evangelist

ZTNA

As no one is to be trusted

Cybersecurity Challenges

Work From Anywhere

"…hybrid work requires a complete revamp of how we think about and approach security. "

eWeek August 2021

Applications are Everywhere

71% of organizations are pursuing a hybrid (36%) or multi-cloud strategy (35%) for integration of multiple services, scalability or business continuity reasons.

2021 Cloud Security Report
Cybersecurity Insiders

Ransomware and Sophisticated Attacks

36% of organizations state the growing sophistication of the threat landscape is the top challenge in preventing ransomware attacks.

Fortinet – Ransomware survey 2021

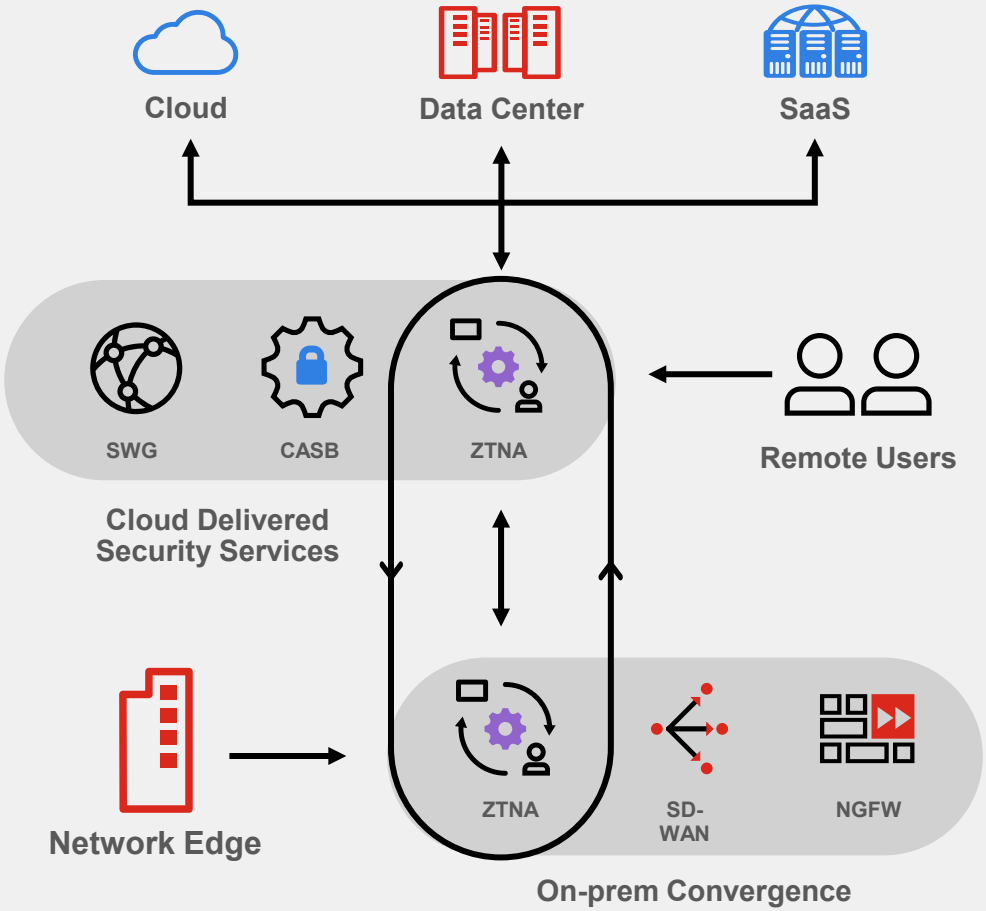
Operational Technology Connectivity

42% indicate that their control systems had direct connectivity to the internet up from 12% in 2019.

SANS 2021 Survey: OT/ICS Cybersecurity, published August 2021

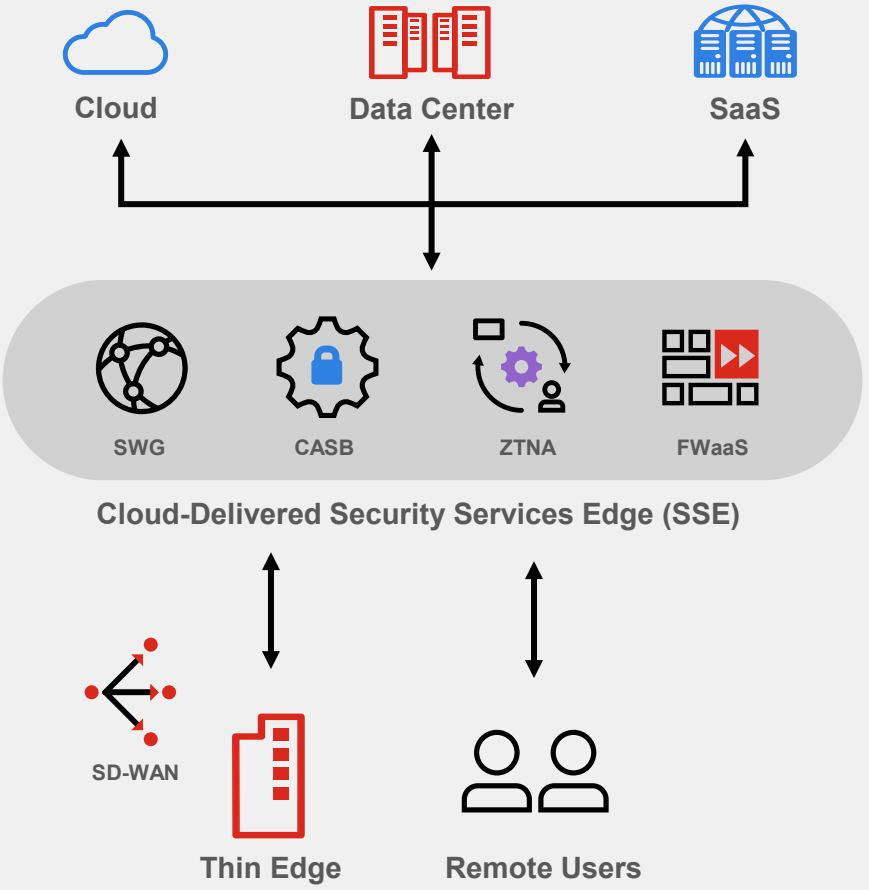
Networking & Security Convergence: Analysts Point of View

Zero Trust Edge



FORRESTER®

SASE



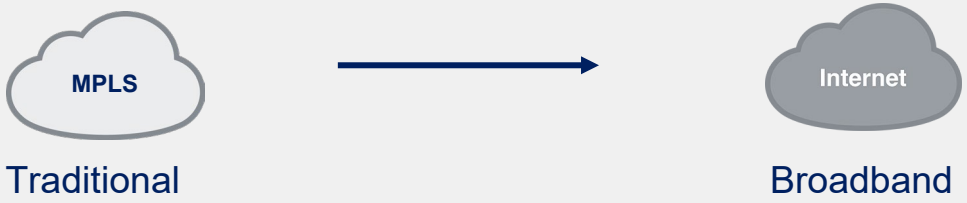
Gartner®

"Digital transformation and accelerating cloud adoption are driving changes in WAN edge infrastructure to be led by IT network and operations leaders responsible for networks"

Gartner

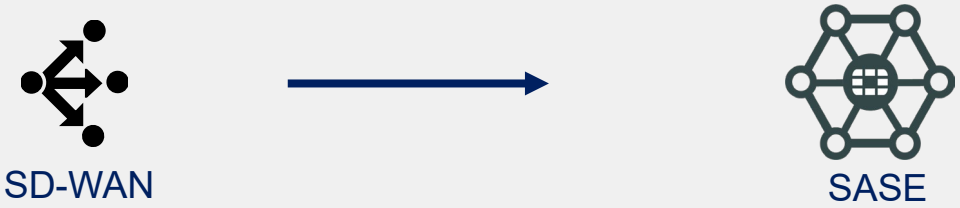
"Consequently, CIO leaders must select SD-WAN vendors that address the changing requirements to connect end users to applications. "

Gartner Strategic Planning Assumptions for WAN Edge



By 2023, to deliver flexible, cost-effective scalable bandwidth, 30% of enterprise locations will have only internet WAN connectivity, compared with approximately 15% in 2020

By 2024, to enhance agility and support for cloud applications, 60% of enterprises will have implemented SD-WAN, compared with about 30% in 2020.



By 2024, more than 60% of software-defined, wide-area network (SD-WAN) customers will have implemented a secure access service edge (SASE) architecture, compared with about 35% in 2020.

By 2024, 20% of SD-WAN centralized configuration and troubleshooting will be touchless via an artificial intelligence (AI) assistant, compared with none in 2020

Gartner: Magic Quadrant for WAN Edge Infrastructure

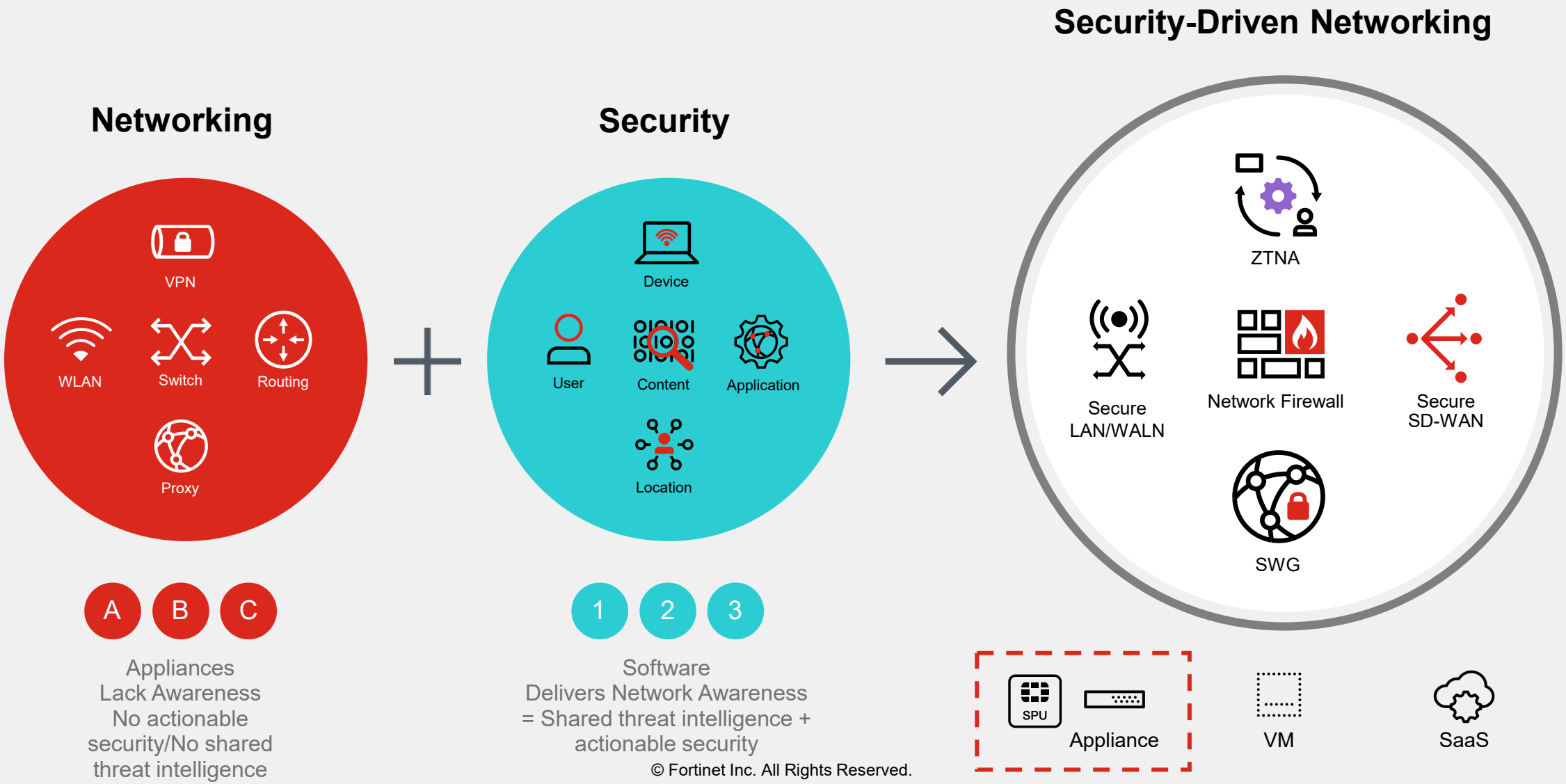
Gartner - MQ WAN Edge 2022

Figure 1: Magic Quadrant for SD-WAN

Source: Gartner (September 2022)

Convergence of Networking and Security

Security-Driven Networking



Users – Devices – Applications & Data - Everywhere

Users & Devices

- Travel 
- WFH 
- Office 
- Plant 

Networks

- Wi-Fi 
- Switch 
- SD-WAN 
- 5G 
- Cloud On Ramp 

Applications

- Cloud 
- Data Center 
- SaaS 
- Edge Compute 

SecOps

- Silo products and technologies 
- Overwhelming alert volume 
- Shortage of cyber security skills 

- High-volume automated attacks 
- Coordinated multi steps attacks 
- Evasive ML-Powered attack tactics 
- Increasing financial and human impact

Ensuring consistent enterprise class security independent of device type & location

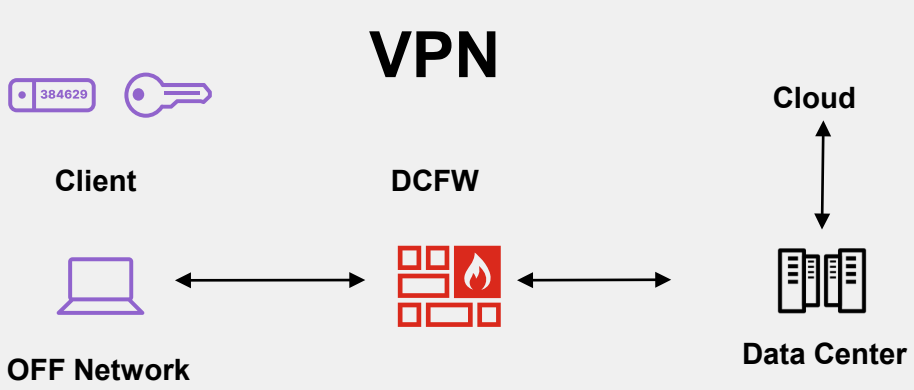
The Perimeter has expanded across the entire network creating more edges which need to be secured

Applications continue to move and are spread across multiple cloud creating complex operational overhead that result in security challenges

The volume of security products and information overwhelms teams chronically short of skilled staff, slowing the ability to detect and respond to incidents

Attackers will continue to innovate leveraging AI driven insights and large scale automated execution across the full attack surface and cycle

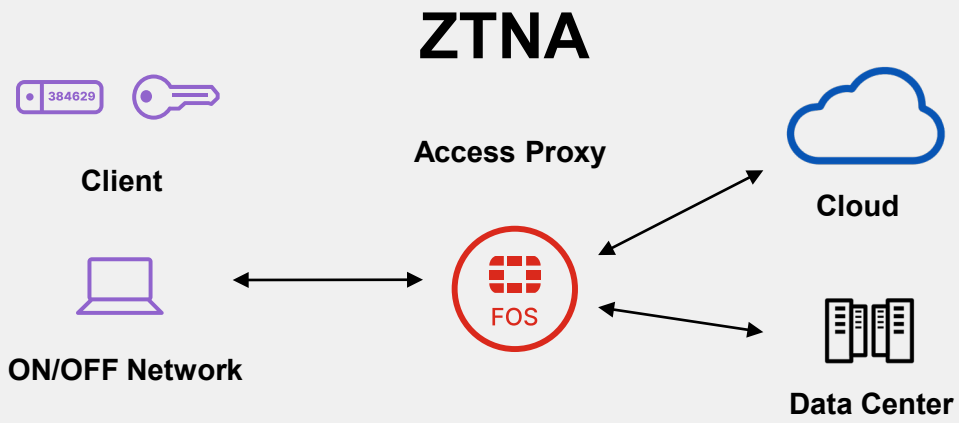
Evolution to ZTNA



One Time Trust Check

Access Entire Network

Generic Rule Set

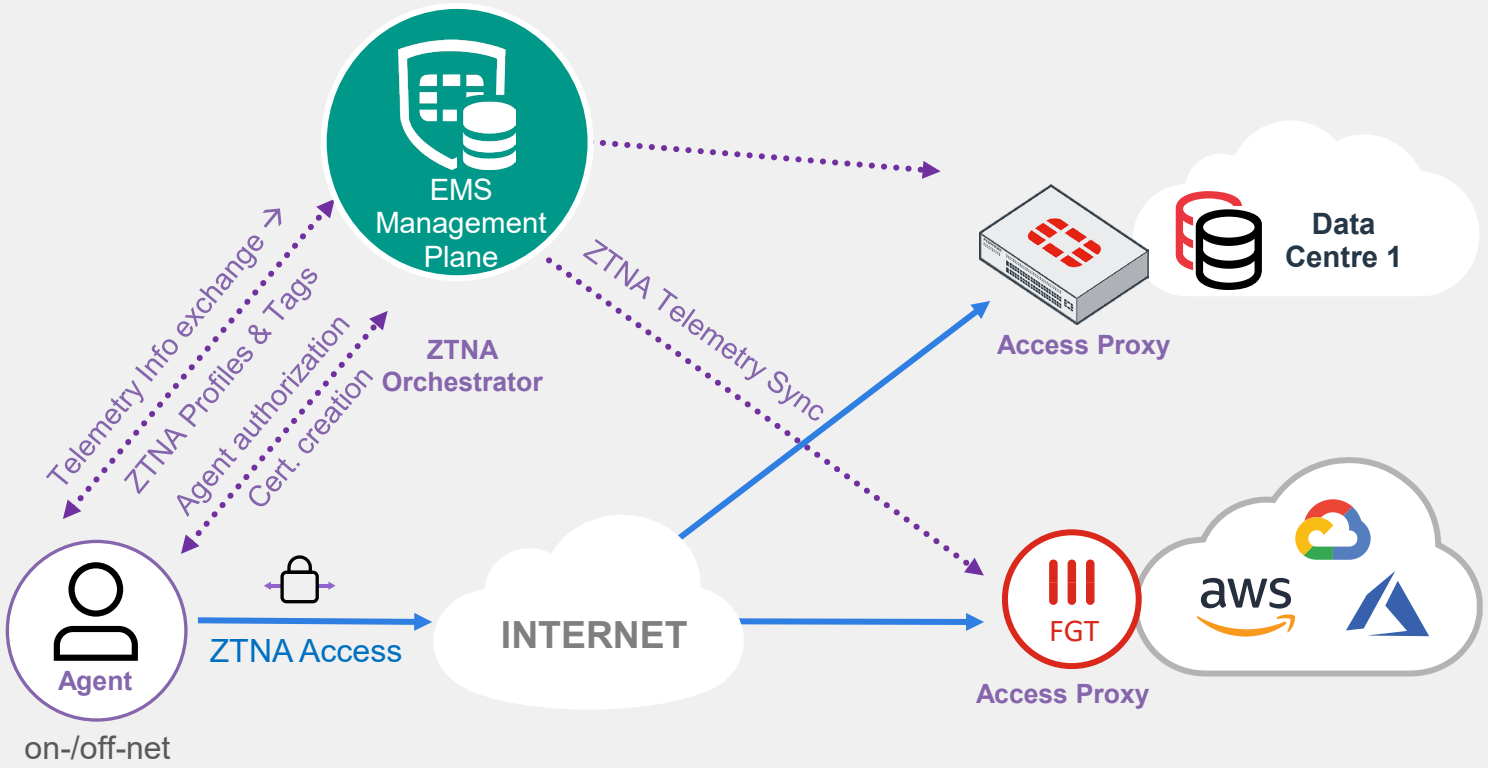


Continuous Trust Check

Access Specific Applications

User Contextual Rule Set

ZTNA Architecture



- **ZTNA Telemetry**
- **Fabric Sync**
- Secure **just enough access**
- **Continuous** posture re-evaluation

Validate Device | Verify User | Device Posture | Application Access Only

per session/application

FortiSASE

… and how it all comes together

FortiSASE Use Cases – Best of two worlds

Secure Access to Internet & SaaS

Remote Users (Work From Anywhere)

- ✓ **Protecting/Controlling remote users when access Internet**
- ✓ **Protecting Company Endpoints from Internet Threats**

License based on endpoints or users

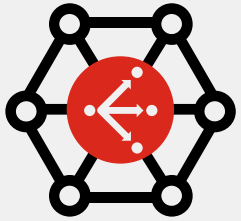
Secure Access to Corporate Apps

Private Access (using ZTNA tags)

- ✓ **SIA (Agent-Based)**
- **+**
- ✓ **Private apps secure access**
- ✓ **Zero Trust Policies**

License based on endpoints or users

Private Access (SD-WAN)**



- ✓ **SIA (Agent-Based)**
- **+**
- ✓ **Private apps secure access**
- ✓ **Zero Trust Policies**
- ✓ **Integration with on-Prem FGTs**

License based on endpoints or users

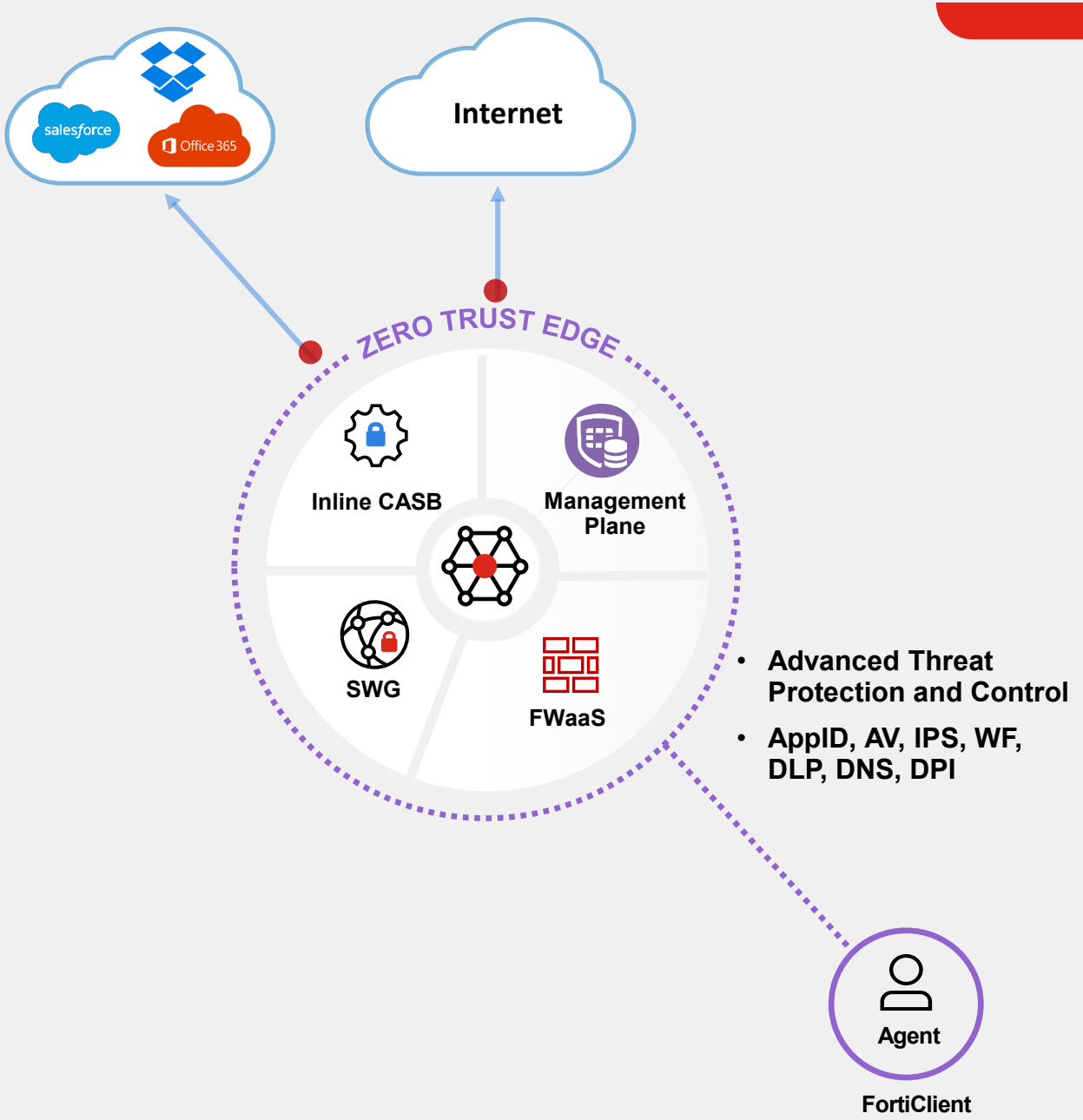
NEW

Secure Internet Access & SAAS

For Remote Users

Agent-Based access with FortiClient:

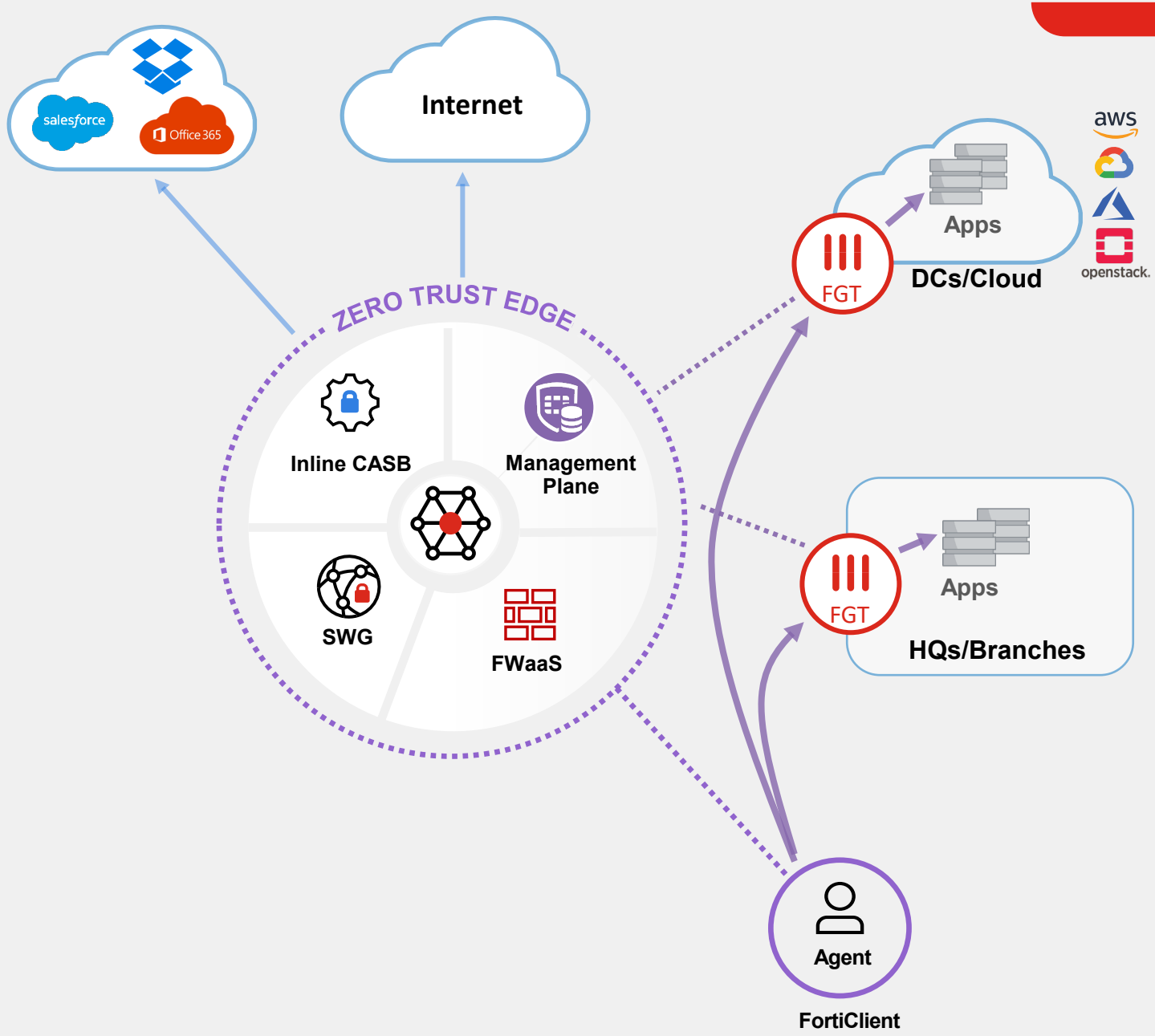
- Unified Endpoint Management
- lightweight agent, no-touch provisioning
- ZTNA Orchestration
- Shared Security profiles for consistent protection



Secure Private Access (on prem applications)

ZTNA Access Proxy

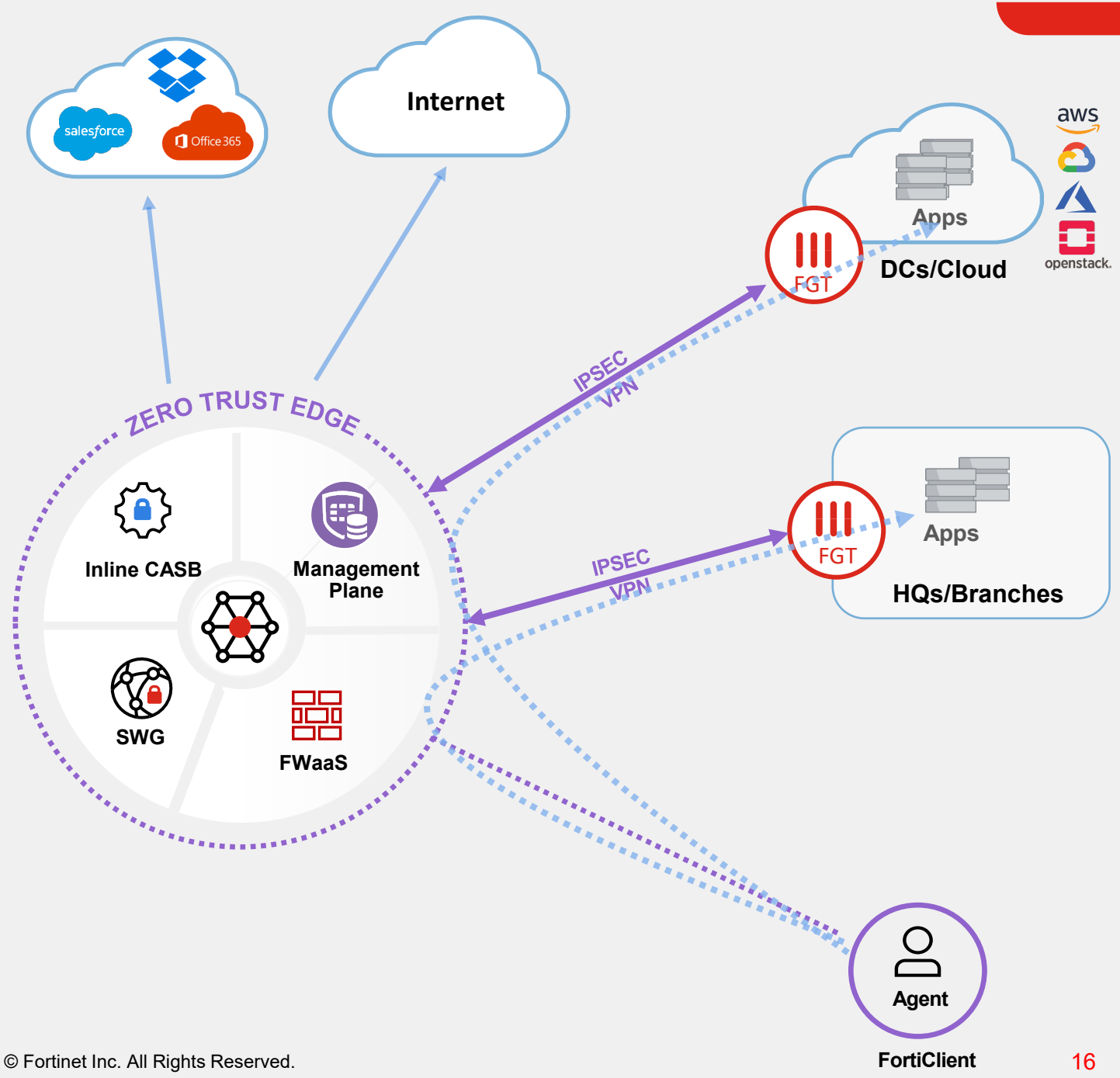
- Auto-on secure ZTNA sessions
- Per-application, per-session authentication
- User contextual policies
- Device posture checks
- Continuous re-assessment and enforcement
- Centrally orchestrated by FortiSASE



Secure Private Access

Network Integration

- **FortiSASE joins Existing FortiGate deployment**
- FortiSASE secures remote users and connects them directly to the applications behind FortiGate(s)
- FortiSASE has SDWAN overlay configuration to balance the traffic among DCs
- Same FOS everywhere!
- Consistent ZTNA & Security across the entire Fortinet ecosytem.



SASE Security PoP Footprint

Global coverage

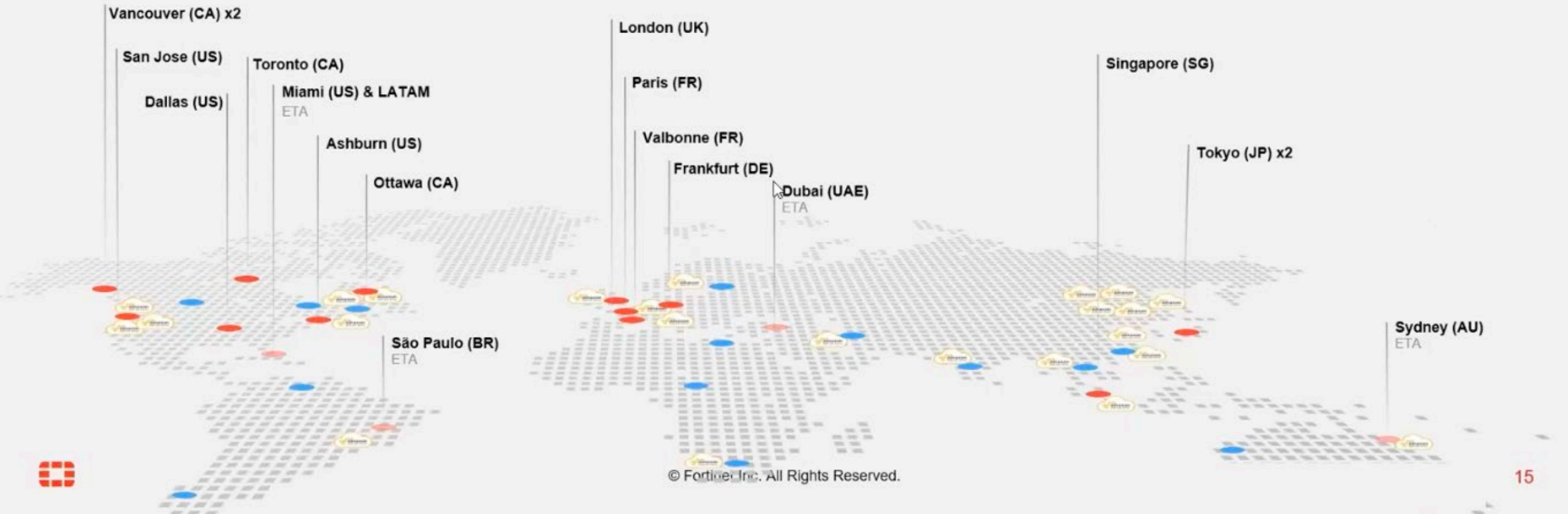
FortiSASE DC Locations
- Available
- In progress
- Planned

Global
Coverage
Global theatres

18
Active Datacenters
Rapid roll out

32
Datacenters by end 2023
Regional coverage

38
AWS FWaaS Datacenters
Extended coverage



Key Differentiators Messages

Flexibility on security consumption	▪ Consume security where it makes most sense to the business (On-prem/VM/Cloud)
Simplified architecture and connectivity	▪ Integrated Branch Office architecture for DIA with secure SD-WAN (branches), ThinEdge (SoHo) and remote users
Consistent Zero Trust security across all users	▪ Same level of Zero Trust security for all users On-Net / Off-Net
Simplified Management	▪ Single OS (FortiOS) operating across all Edges and running natively ZTNA capabilities ▪ Centralized Orchestration for ZTNA policies (coming soon)
Centralized Visibility and Monitoring	▪ Native Integration with FortiAnalyzer to provide unified visibility and monitoring
Simplified Licensing	▪ All-in-one license for remote users (no add-ons)

Three Key Takeaways

A journey towards the creation of full Zero Trust service

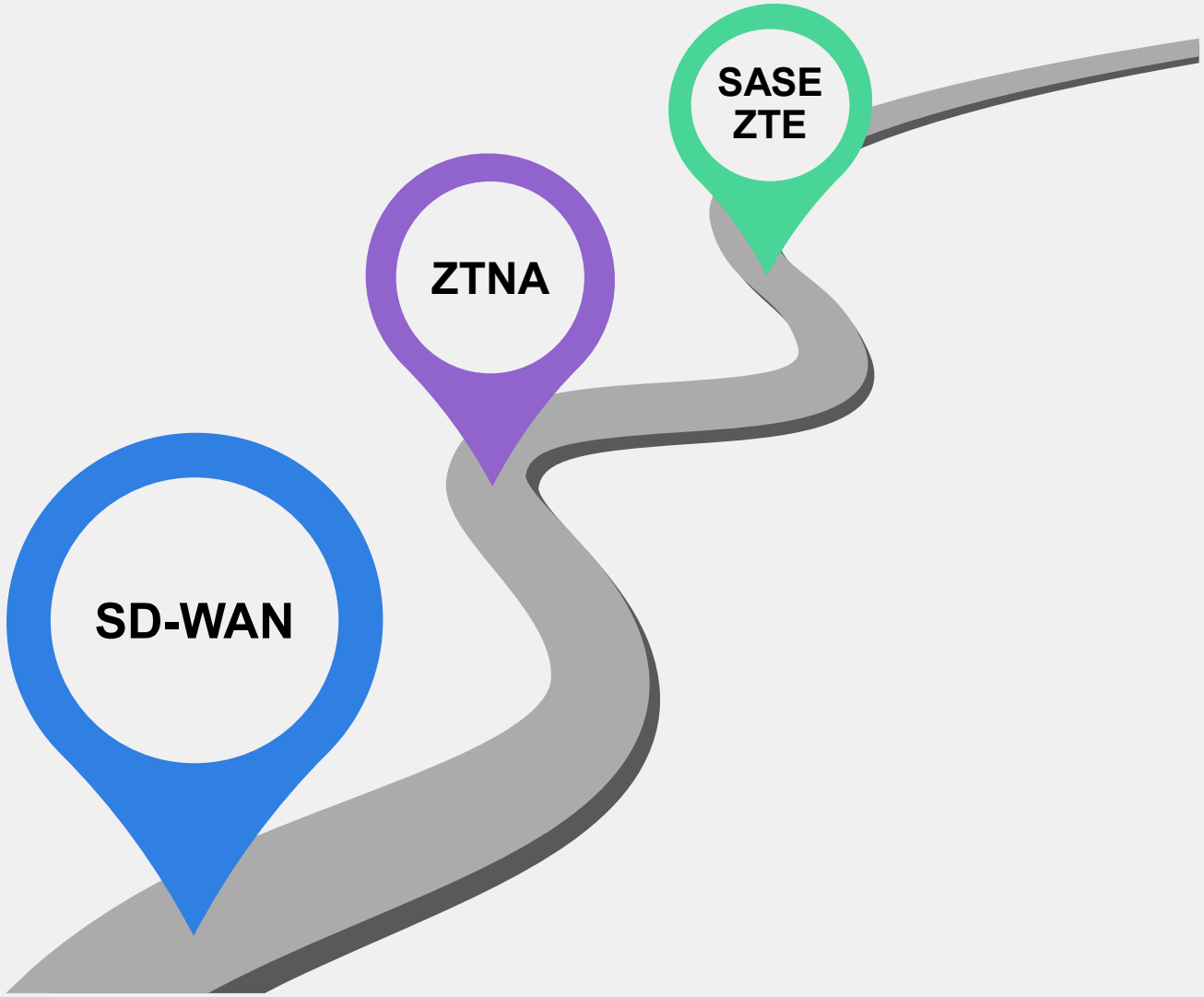
- Modularity of offering
- Enabling various starting point

The hybrid approach is the most compelling solution

- Matching different use cases, geography, and maturity
- Delivering a consistent user experience

This is only the start of the journey

- Fortinet Security Fabric




FORTINET