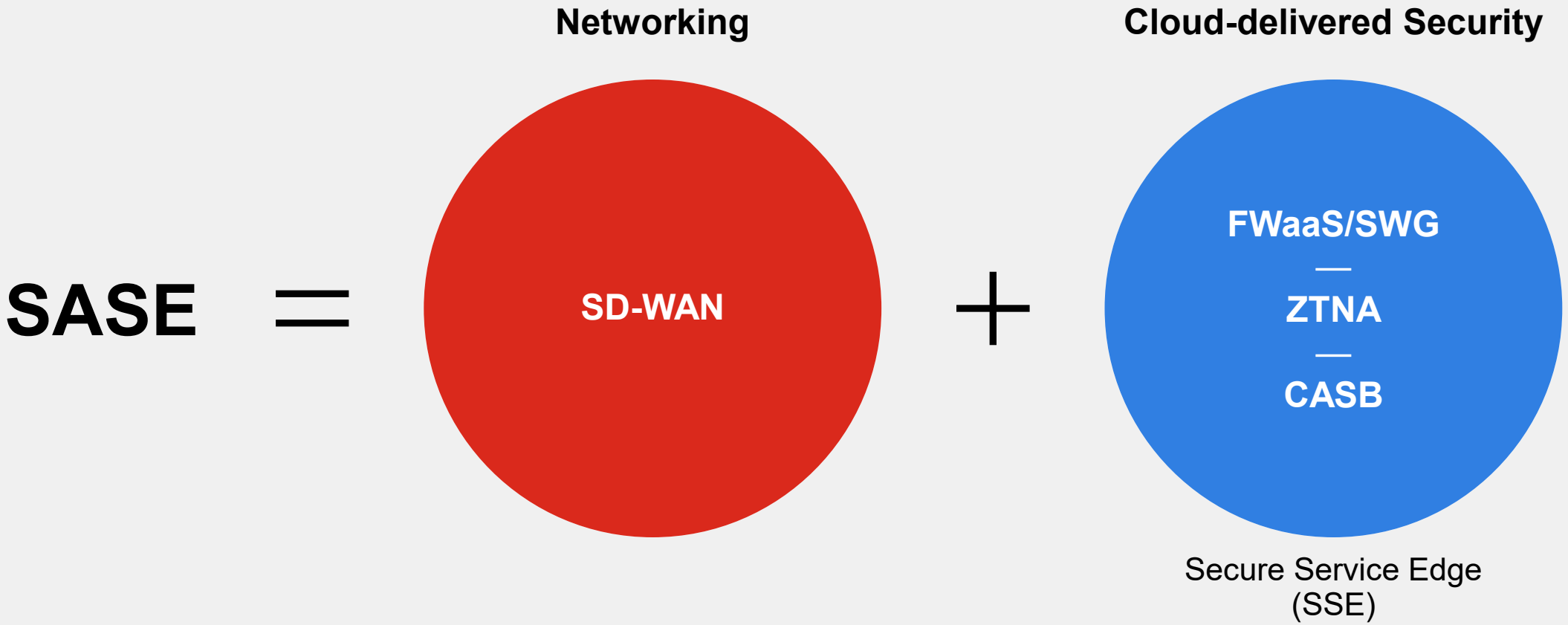
Demystifying SASE

Ahto Tomingas

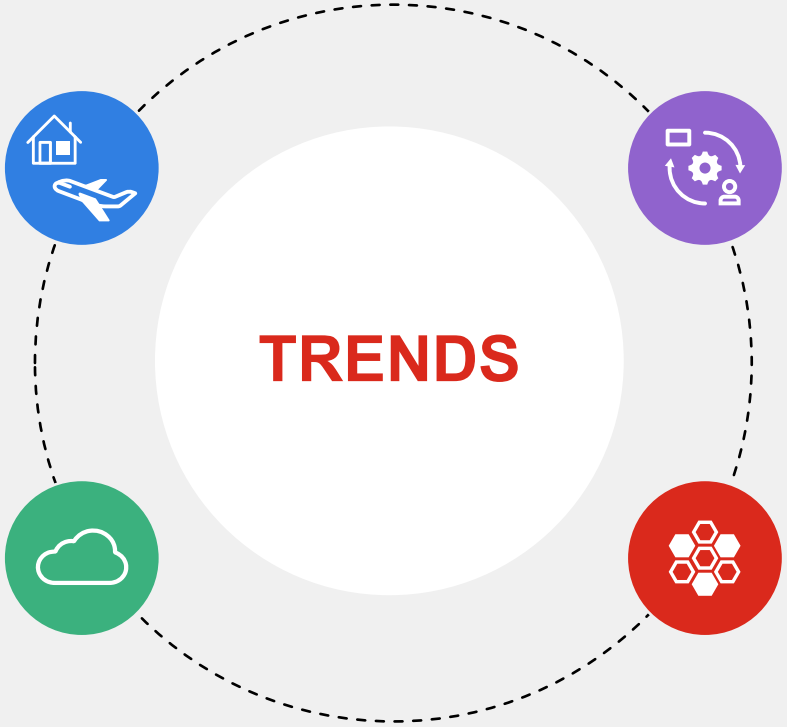
Sr. Systems engineer, SecOps Lead, Baltics

What is SASE (Secure Access Service Edge)?

Cloud-delivered network and security convergence solution for work-from-anywhere



Market Trends driving SASE adoption



Hybrid workforce
94% of organizations are allowing employees more flexibility as to where and when they work

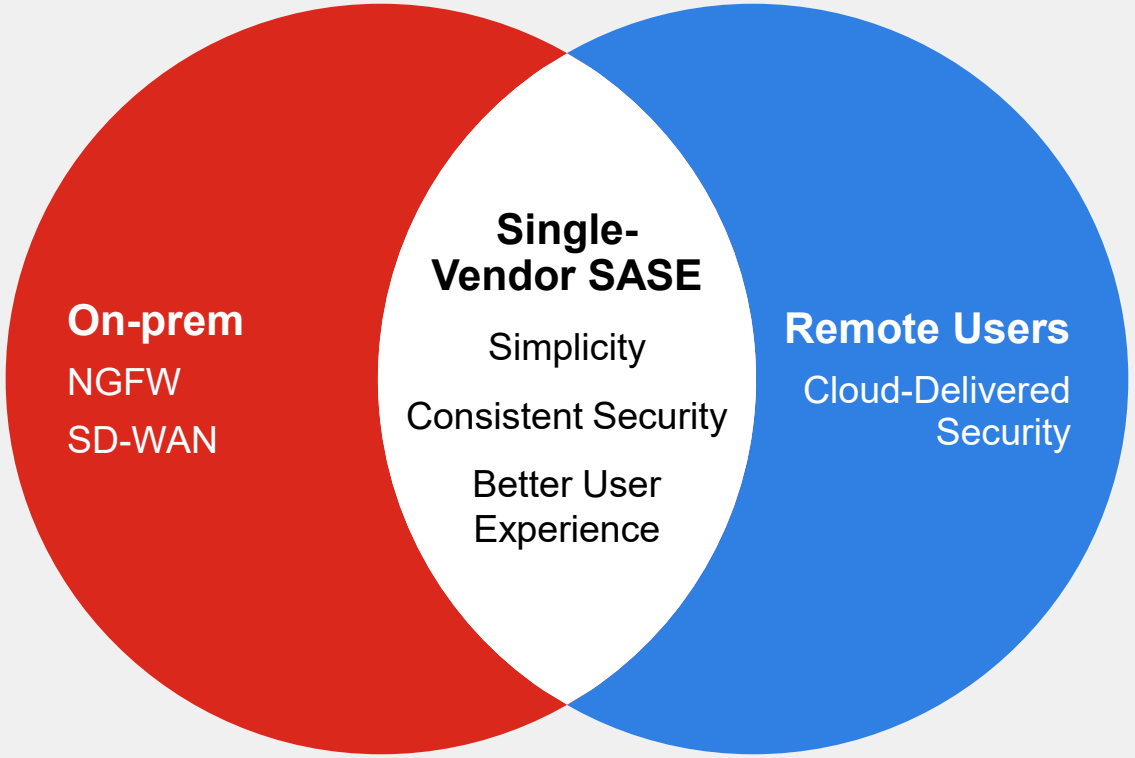
From VPN to ZTNA
By 2025 at least **70%** of new remote access deployments will rely on ZTNA rather than VPN services

SaaS adoption
SaaS makes up the largest share of the cloud service market and more than **50%** of the overall software market

Vendor consolidation
75% of Organizations Are Pursuing Security Vendor Consolidation in 2022

https://www.gartner.com/en/human-resources/trends/how-organizations-are-supporting-a-hybrid-workforce
https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i#
https://www.gartner.com/en/digital-markets/insights/saas-growth-strategy
https://www.gartner.com/en/newsroom/press-releases/2022-09-12-gartner-survey-shows-seventy-five-percent-of-organizations-are-pursuing-security-vendor-consolidation-in-2022

Convergence of On-Prem and Remote Users Network



Single-vendor SASE Benefits

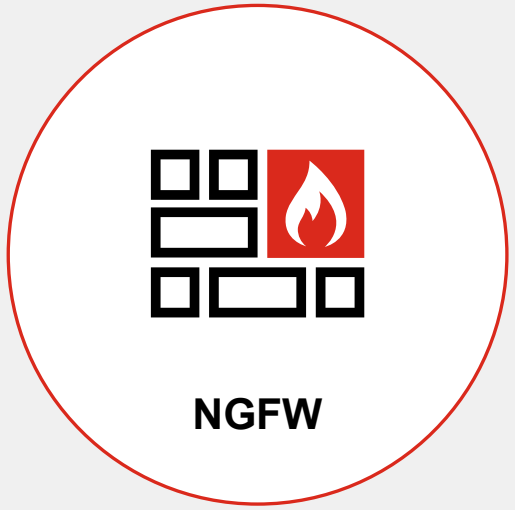
- Improved risk posture and reduced security gaps
- Provide simplicity eliminating multiple products
- Efficient operations with single agent
- Cost savings from product and vendor reduction

Pragmatic Journey to SASE

With Fortinet's convergence of security and networking everywhere

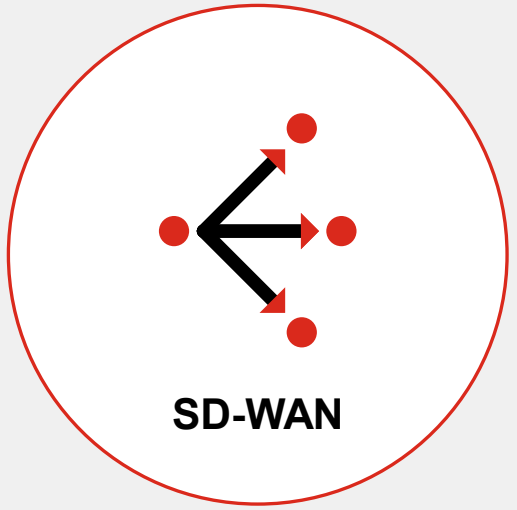
1

Secure Edge Connectivity



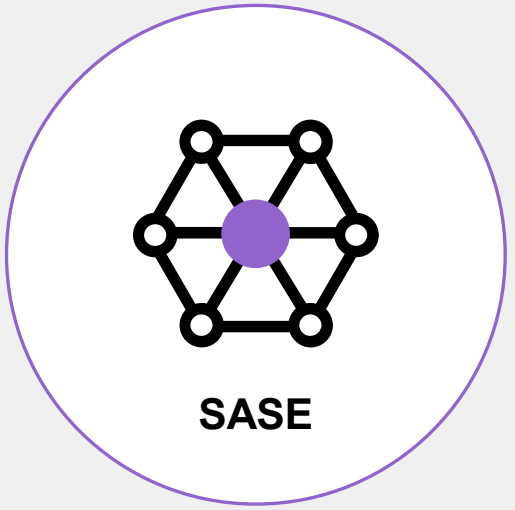
2

Optimize Application Experience

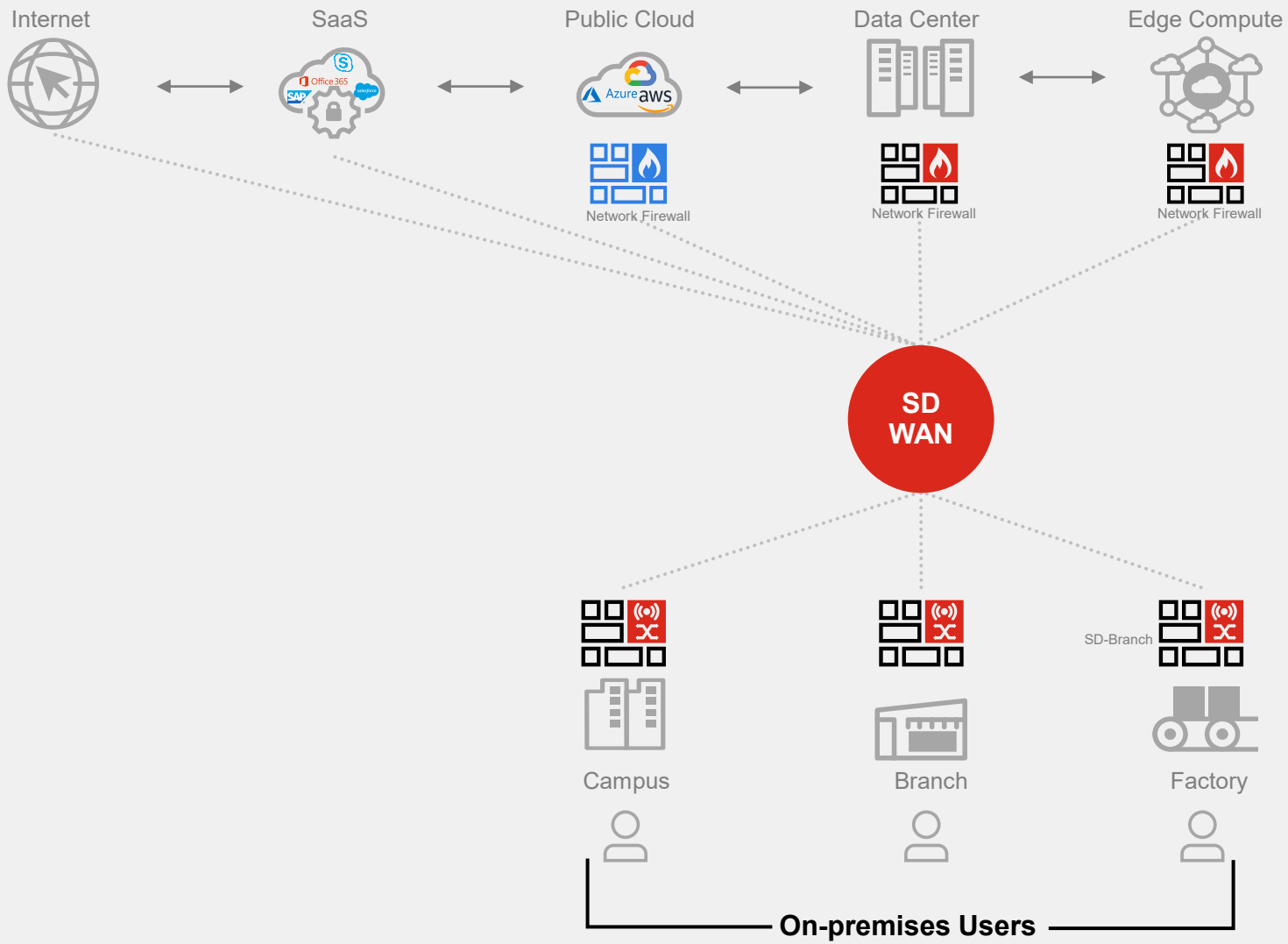


3

Secure Remote Users



Secure SD-WAN : Flexible Application Steering at Edge



Convergence

- Network Firewall
- Secure SD-WAN
- SD-Branch

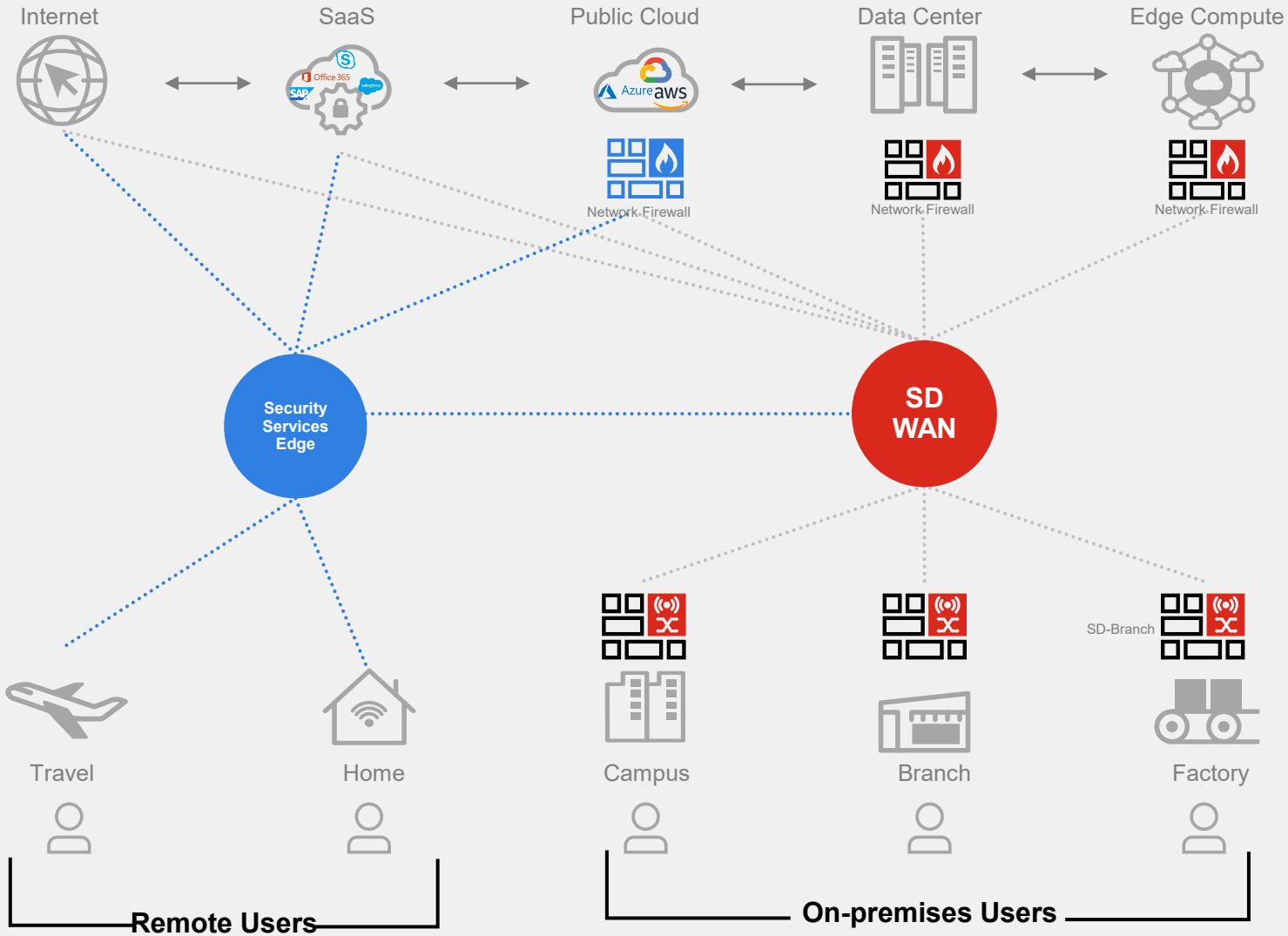
Consistent Security

- Application Aware
- Intrusion Prevention
- Web Filtering
- DNS Protection
- Sandboxing
- In-Line Sandboxing
- In-Line CASB
- OT and IoT Security

Secure Remote Access – Securely connect remote users

Convergence

- Network Firewall
- Secure SD-WAN
- SD-Branch
- Security Services Edge



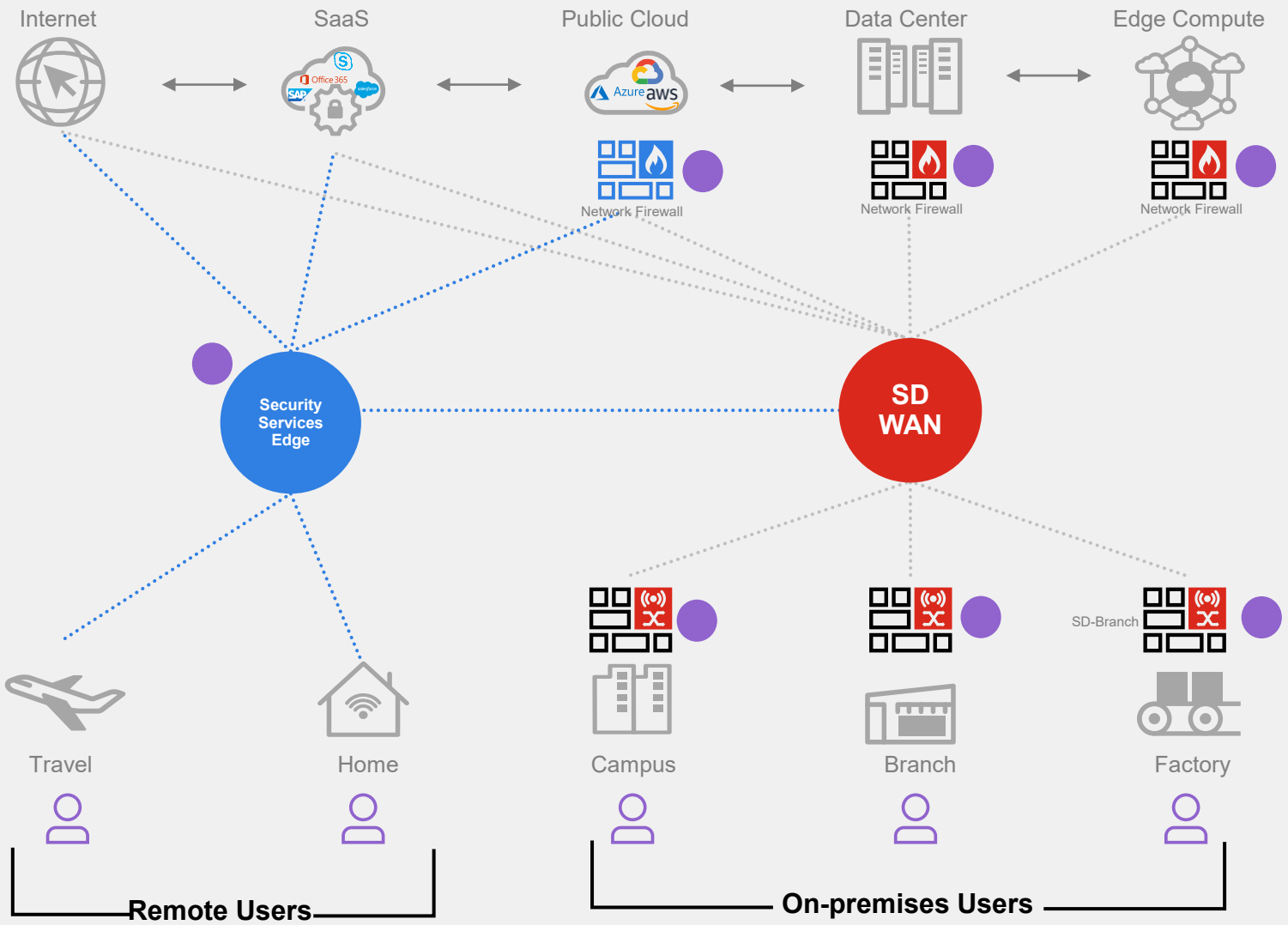
Consistent Security

- Application Aware
- Intrusion Prevention
- Web Filtering
- DNS Protection
- Sandboxing
- In-Line Sandboxing
- In-Line CASB
- OT and IoT Security

Universal ZTNA – Secure user access to applications

Convergence

- Network Firewall
- Secure SD-WAN
- SD-Branch
- Security Services Edge
- Universal ZTNA

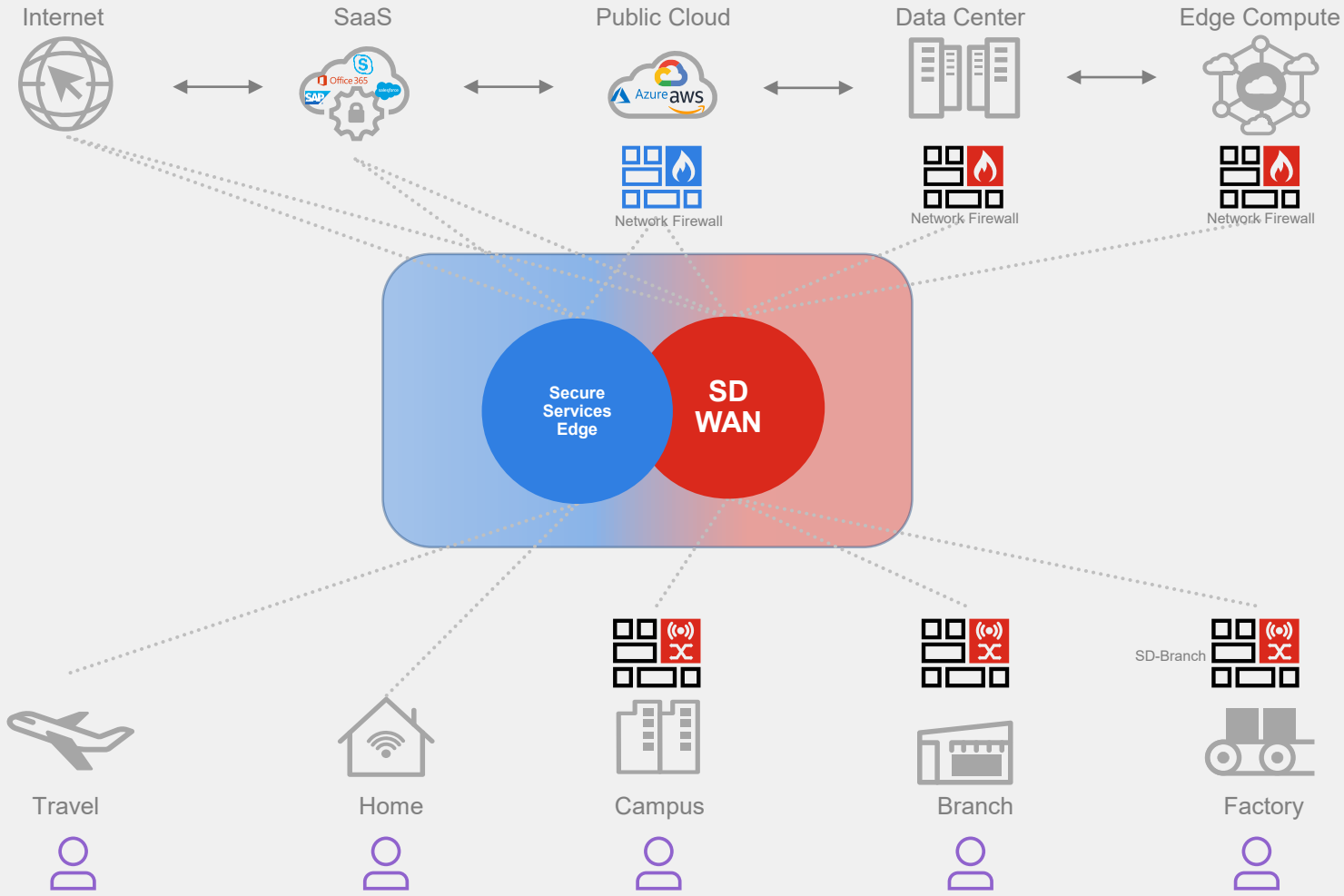


Consistent Security

- Application Aware
- Intrusion Prevention
- Web Filtering
- DNS Protection
- Sandboxing
- In-Line Sandboxing
- Network Access Control (NAC)
- OT and IoT Security

Single Vendor SASE

Converging Remote Users and On-Premises Network



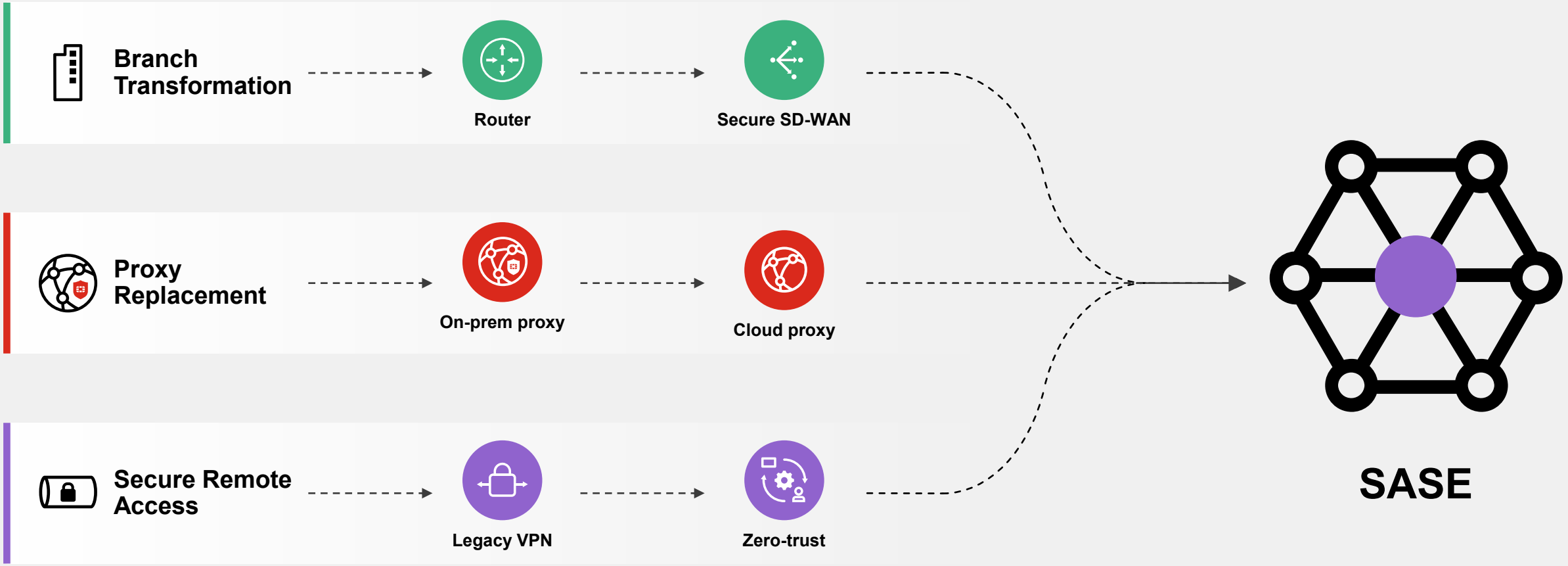
Convergence

- Network Firewall
- Secure SD-WAN
- SD-Branch
- Security Services Edge
- Universal ZTNA

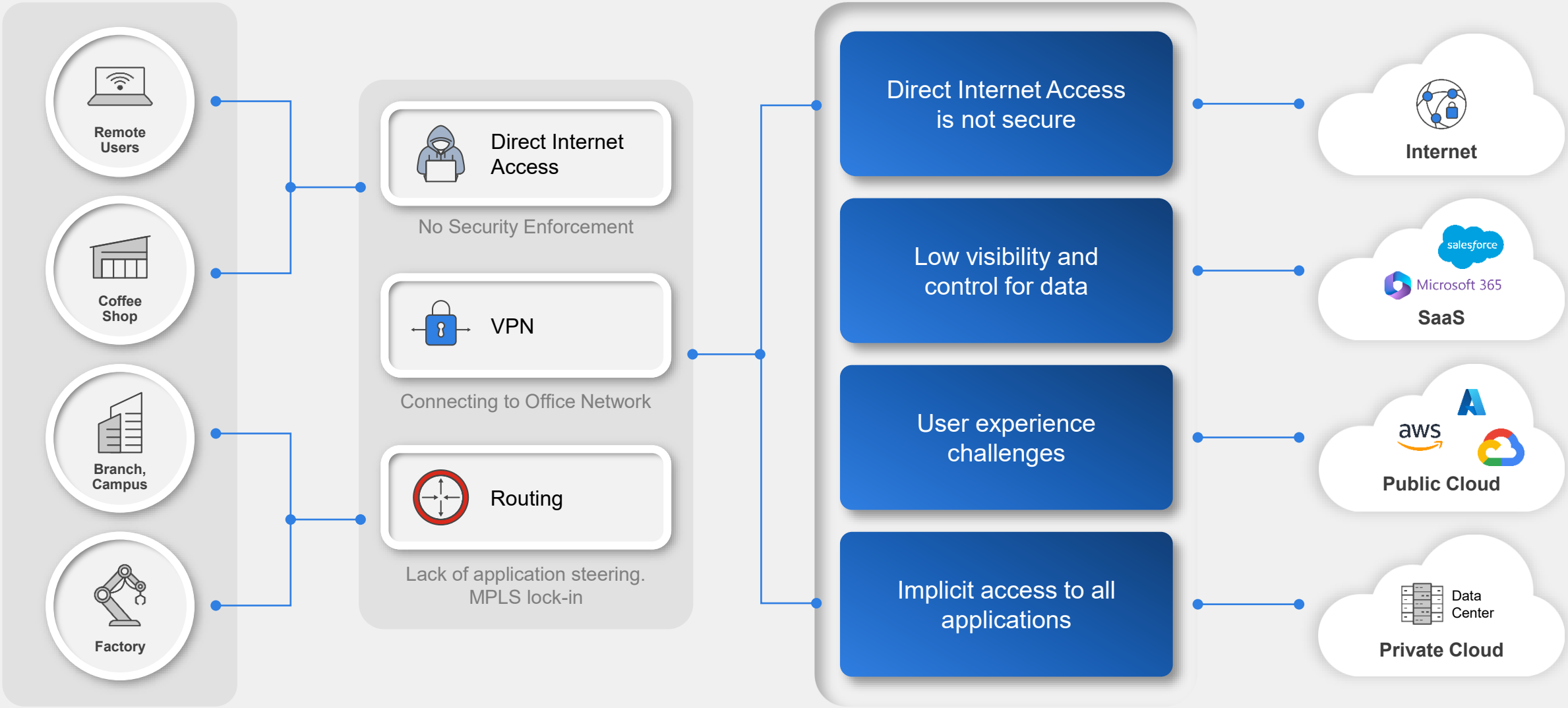
Consistent Security

- Application Aware
- Intrusion Prevention
- Web Filtering
- DNS Protection
- Sandboxing
- In-Line Sandboxing
- Network Access Control (NAC)
- OT and IoT Security

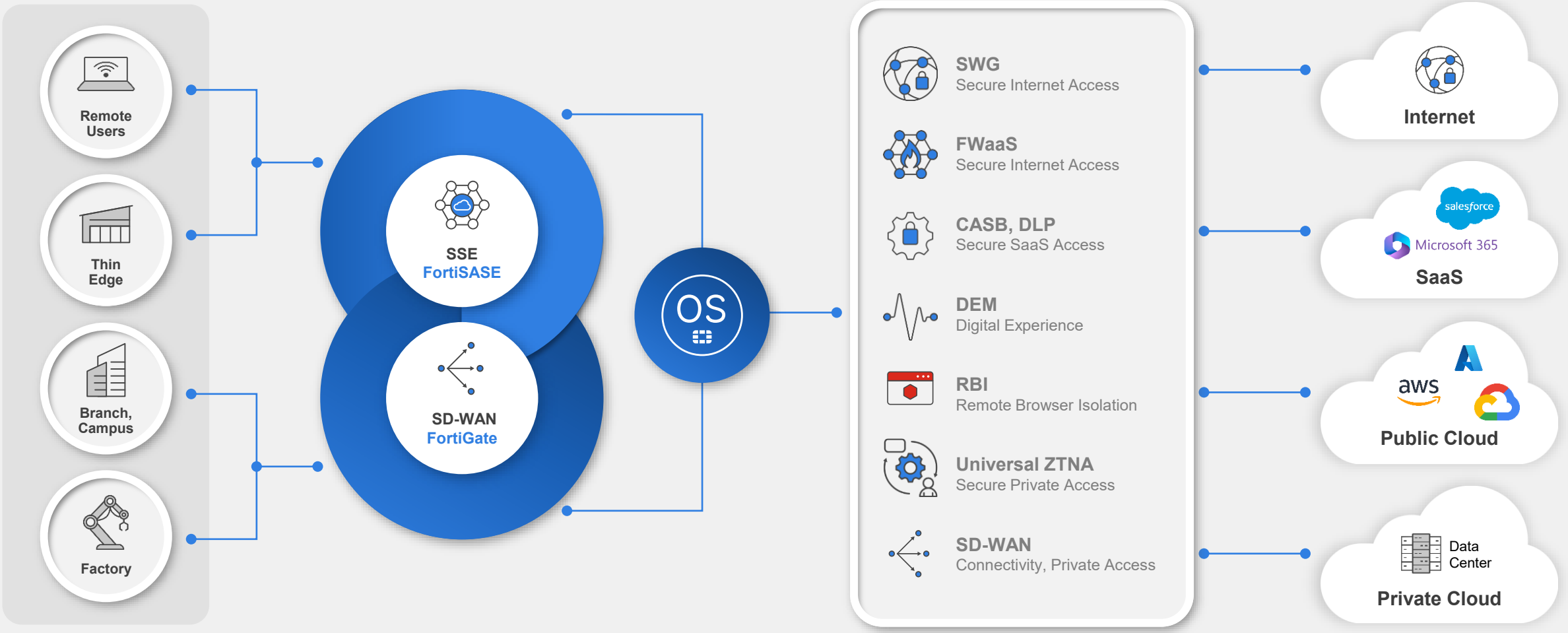
Key Customer Initiatives for SASE



Customer Challenges to Enable Secure Access



Fortinet's Unified SASE Solution for Secure Access



Unified Console, Agent, Data-lake

Flexible Enforcement, Connectivity

AI-Powered Intelligence

Foundation of Unified SASE

ONE OPERATING SYSTEM	UNIFIED MANAGEMENT PLANE	ONE ANALYTICS ENGINE	UNIFIED ENDPOINT AGENT
Single OS	**Central Management**	**Integration with SOC**	**Single agent**
SD-WAN, SSE, NGFW, ZTNA	SSE, SD-WAN, ZTNA	Data lake for security operations	EPP, SASE, ZTNA, CASB, DEM

AI-Driven Security Services with Flexible Consumption

GenAI integration

GenAI security (SSE) & GenAI assistant (SDWAN)

FortiGuard Labs

AI-Driven Security Services

FortiSASE Global Infrastructure

Global Coverage
$1B+ Investment in Infrastructure

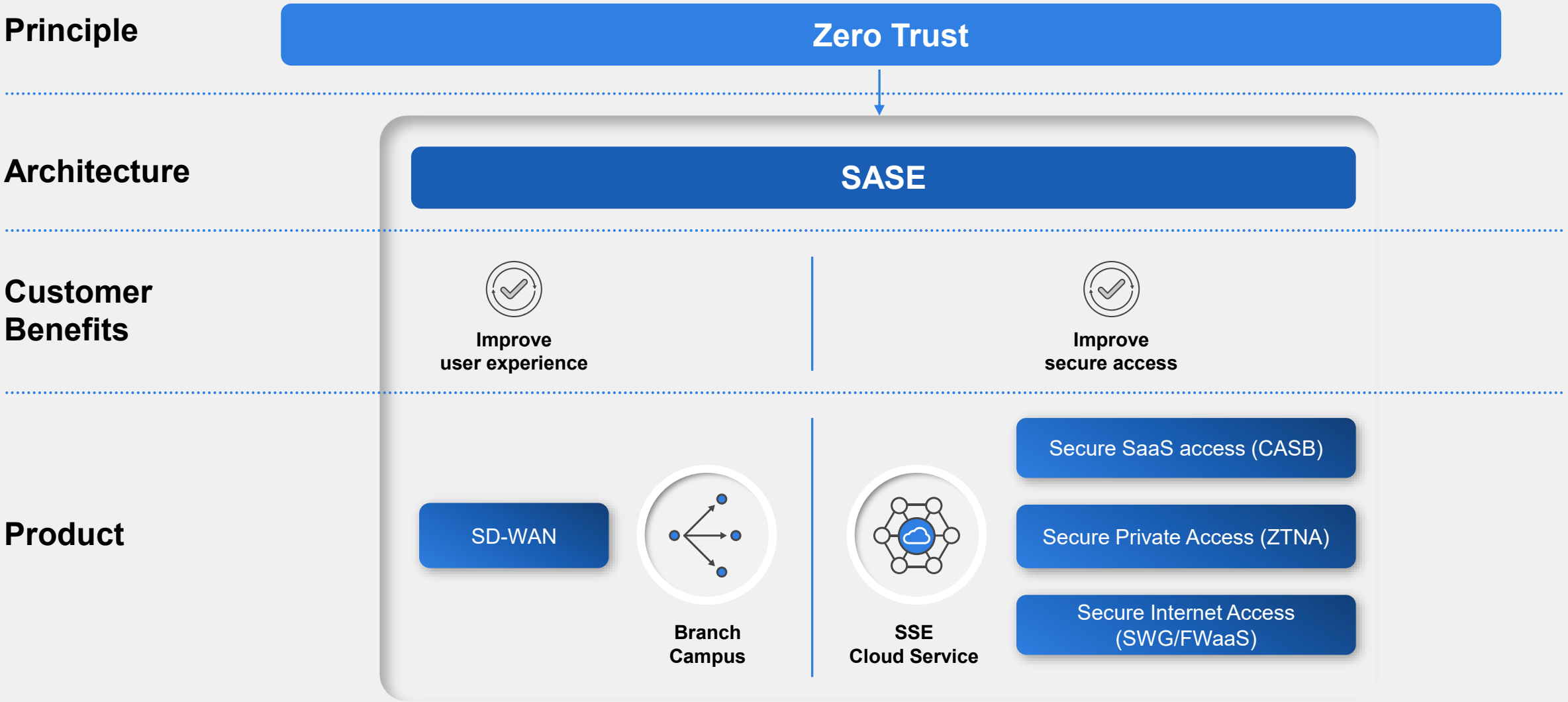
3.3M+ Owned
1.0M+ Leased
4.3M+ Total Sq Ft

160+ Cloud Locations
superior user experience

FortiStack
Organically built integrated solutions

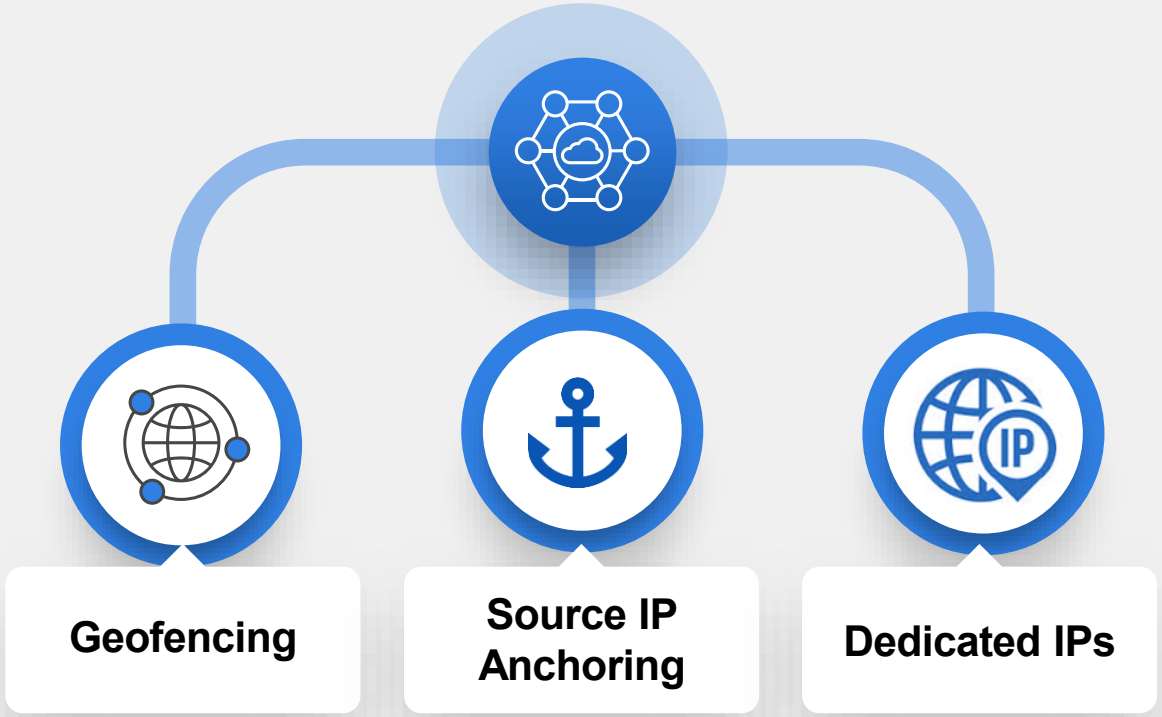
Cost Savings Drive Competitive Advantage

SASE: A Solution to Simplify and Enable Secure Access



- **SWG = Secure Web Gateway / FWaaS = Firewall-as-a-Service**, which protect users and devices from web-based threats.
- **ZTNA = Zero Trust Network Access**, providing secure, identity-based access with explicit control. Can also be sold standalone.
- **CASB = Cloud Access Security Broker**, which ensures secure access to SaaS applications and safeguards sensitive data.

Key infrastructure capabilities for data protection & compliance



Key features

Geofencing

Control the countries from which remote users are allowed to connect to FortiSASE.
Used for data sovereignty.

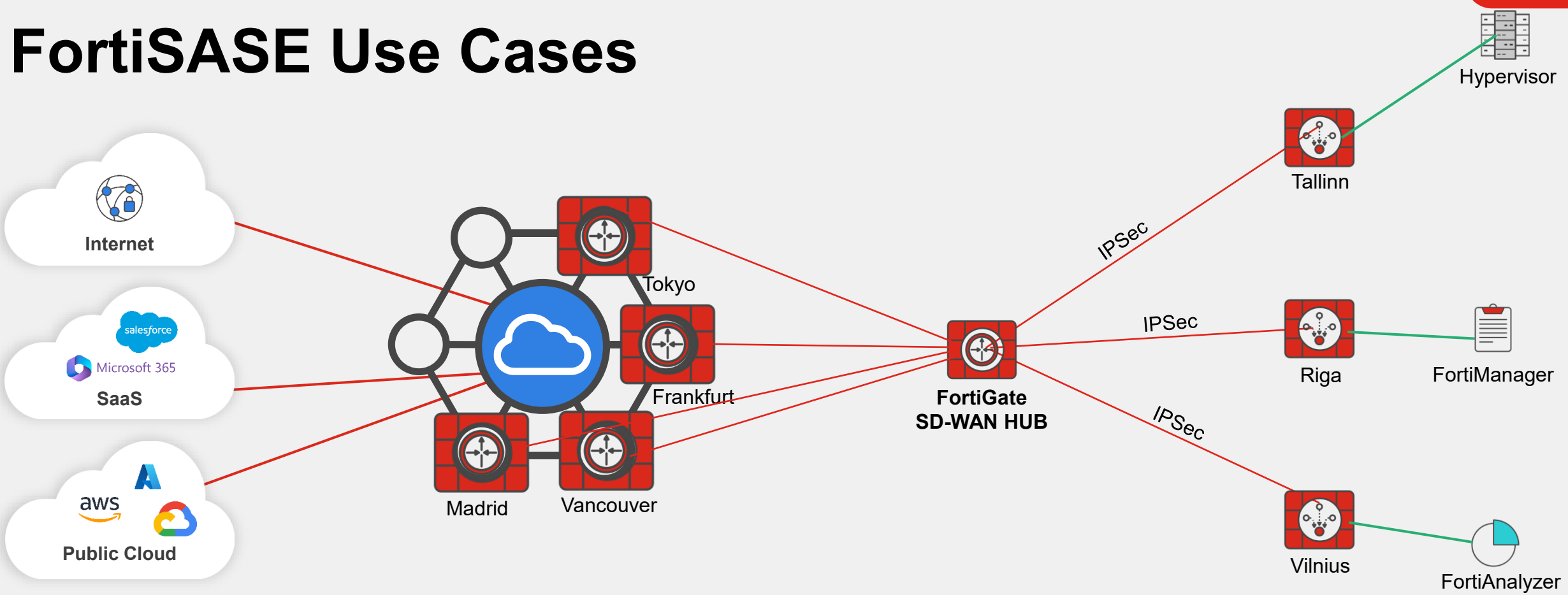
Source IP Anchoring

Ensure that traffic from a user or device appears to originate from a consistent, designated IP address, regardless of their actual physical or network location.
Ideal for regulatory compliance.

Dedicated IPs

Reserved IP addresses to whitelist access from POP to SaaS applications. Ideal for regulatory compliance and threat protection.

FortiSASE Use Cases



FortiSASE SIA

Enable secure web browsing for remote users to protect from known and unknown threats

FortiSASE SSA

Address Shadow IT visibility challenges by deploying SaaS application control and safeguard data loss prevention

FortiSASE SPA

Explicit application access under a zero-trust access or with SD-WAN integration to ensure secure application access

Secure Internet Access

For Remote Users, Thin Edge and Branch Locations

Flexible steering methods

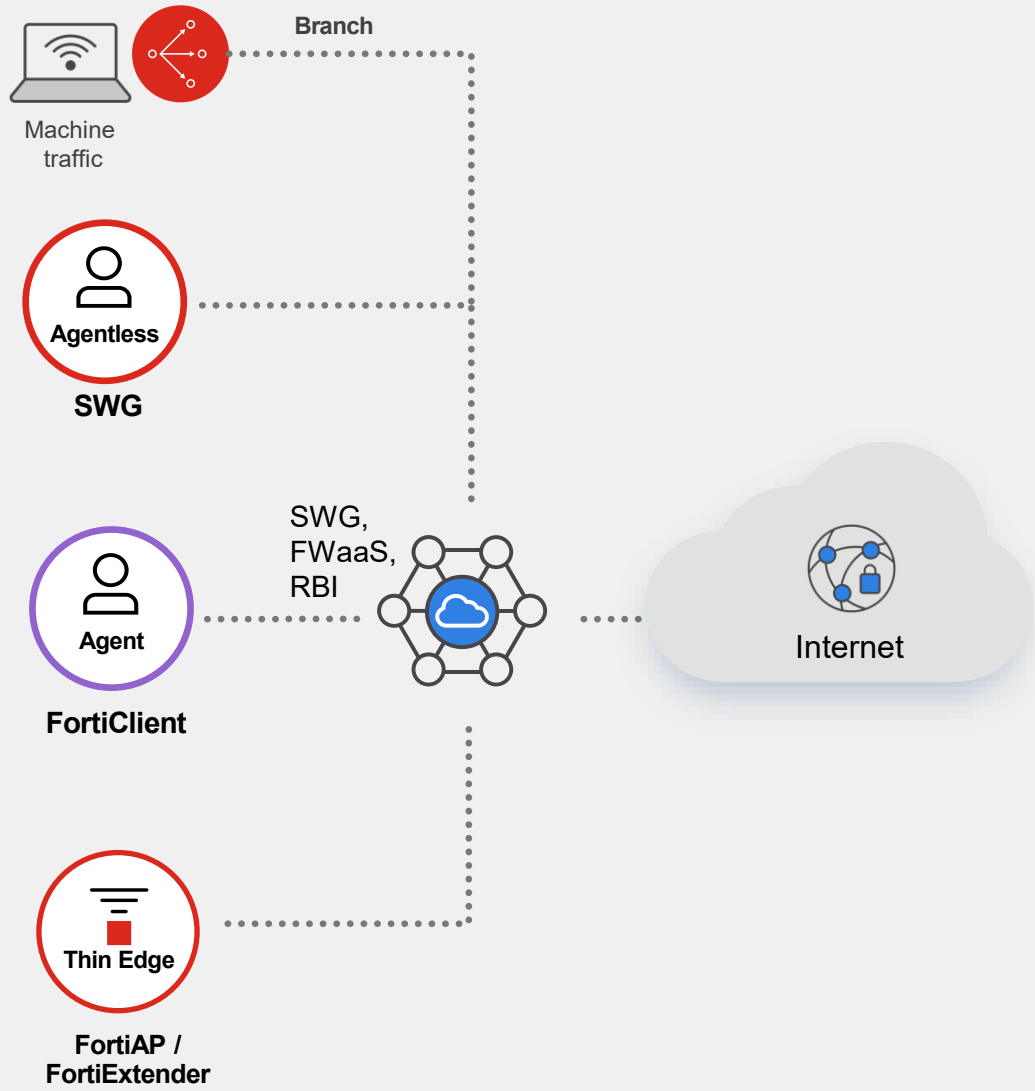
Agent, agentless, thin edge and branch access. Branch access can be either through a 3rd party router or a FortiGate.

Malware & Ransomware prevention

Prevent threats with cloud-based Firewall, IPS, Web Filtering, Anti-virus, DNS and File Filtering, Sandbox, RBI

Full Threat Protection

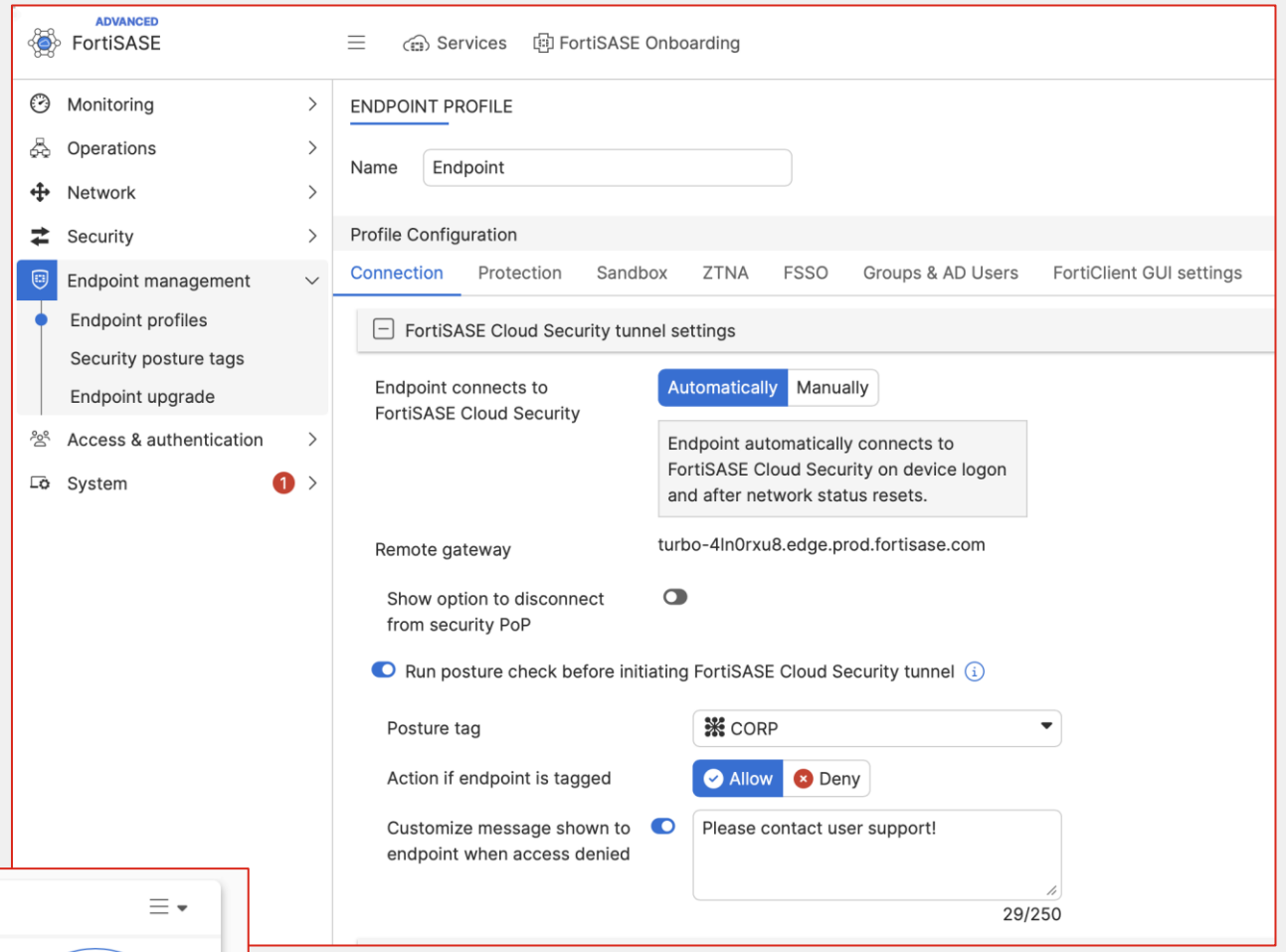
Deep SSL inspection of web & SaaS apps for threats,
Best in class security efficacy and zero-day threat protection with AI powered FortiGuard Security Services

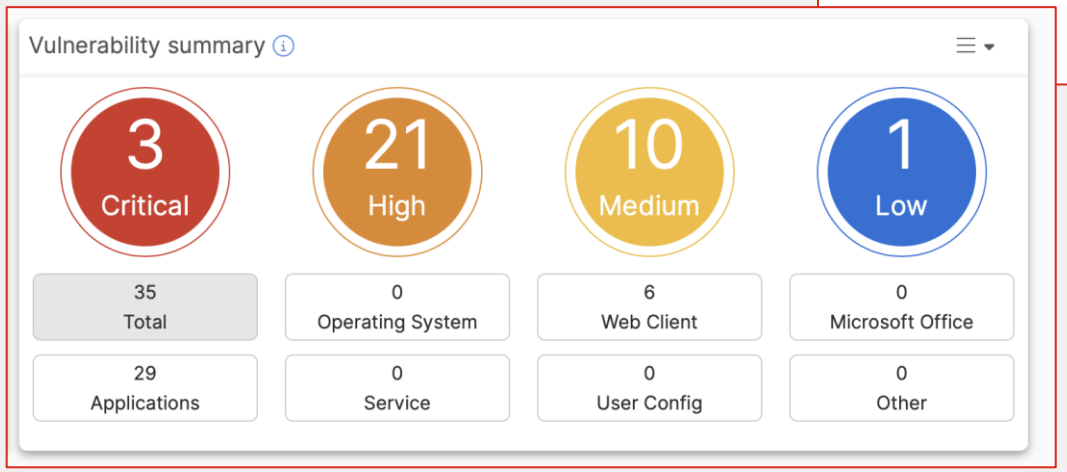


Unified Agent - FortiClient

Unified agent

- VPN client
- Zero Trust Network Access (ZTNA)
- Next Generation AntiVirus
- Anti-Ransomware
- Vulnerabilities scan
- Removable media access control
- Sandbox
- Digital experience monitoring





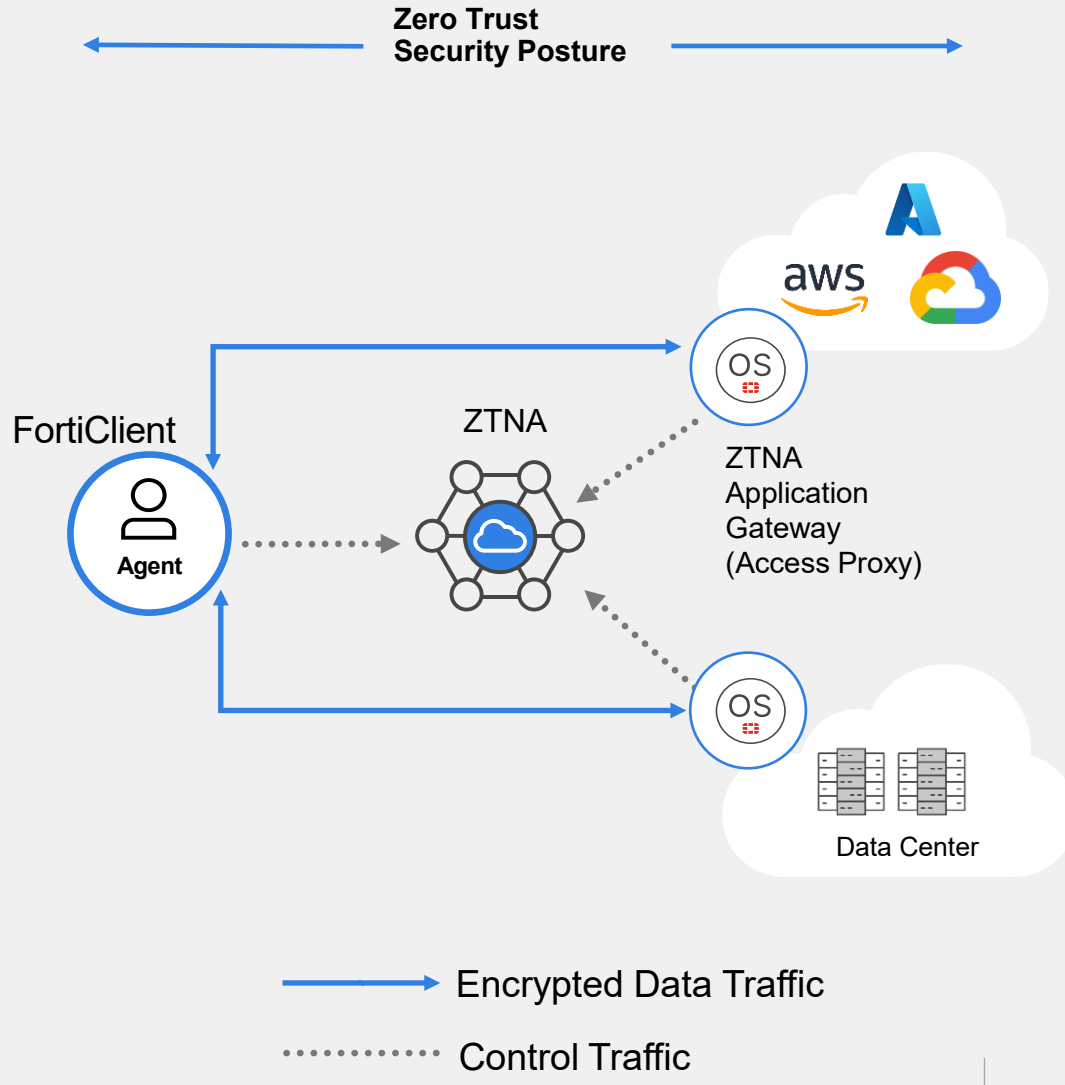
Secure Private Access with ZTNA

FortiSASE ZTNA Support

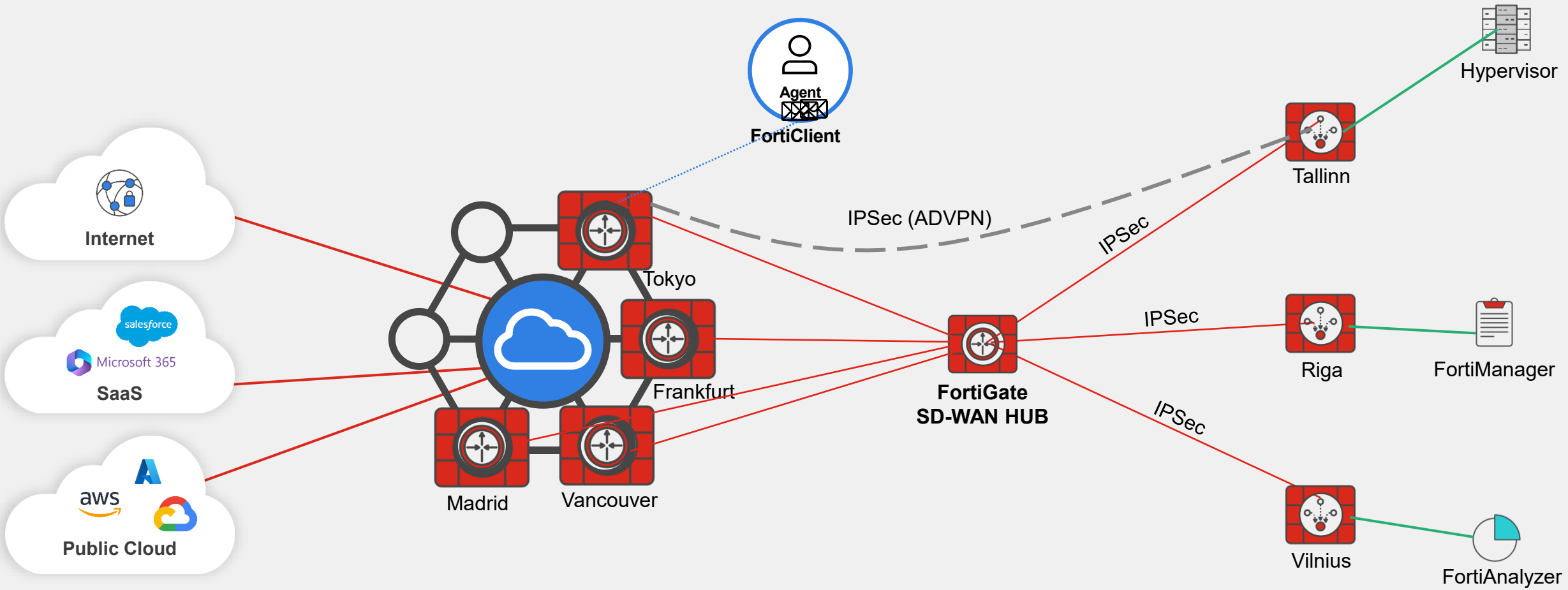
100% Data Privacy! No SSL Inspection on POP

Fastest Routing, **no by-pass** via POP required

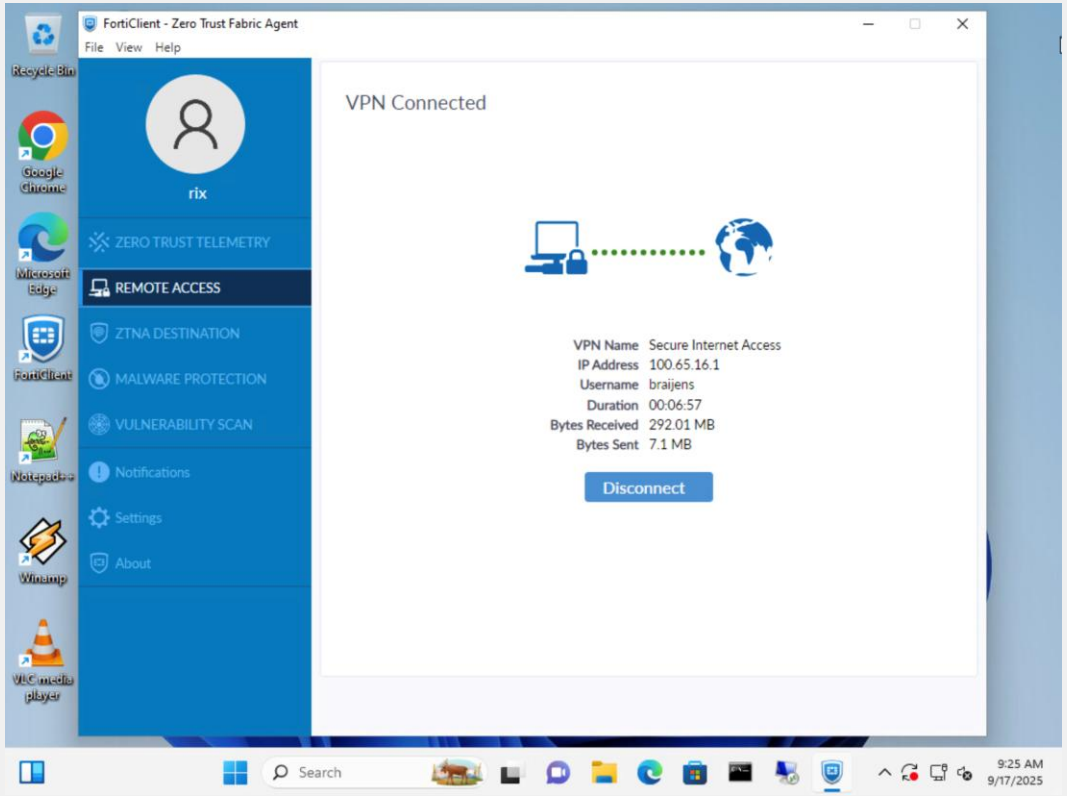
Full FortiGuard AI Security

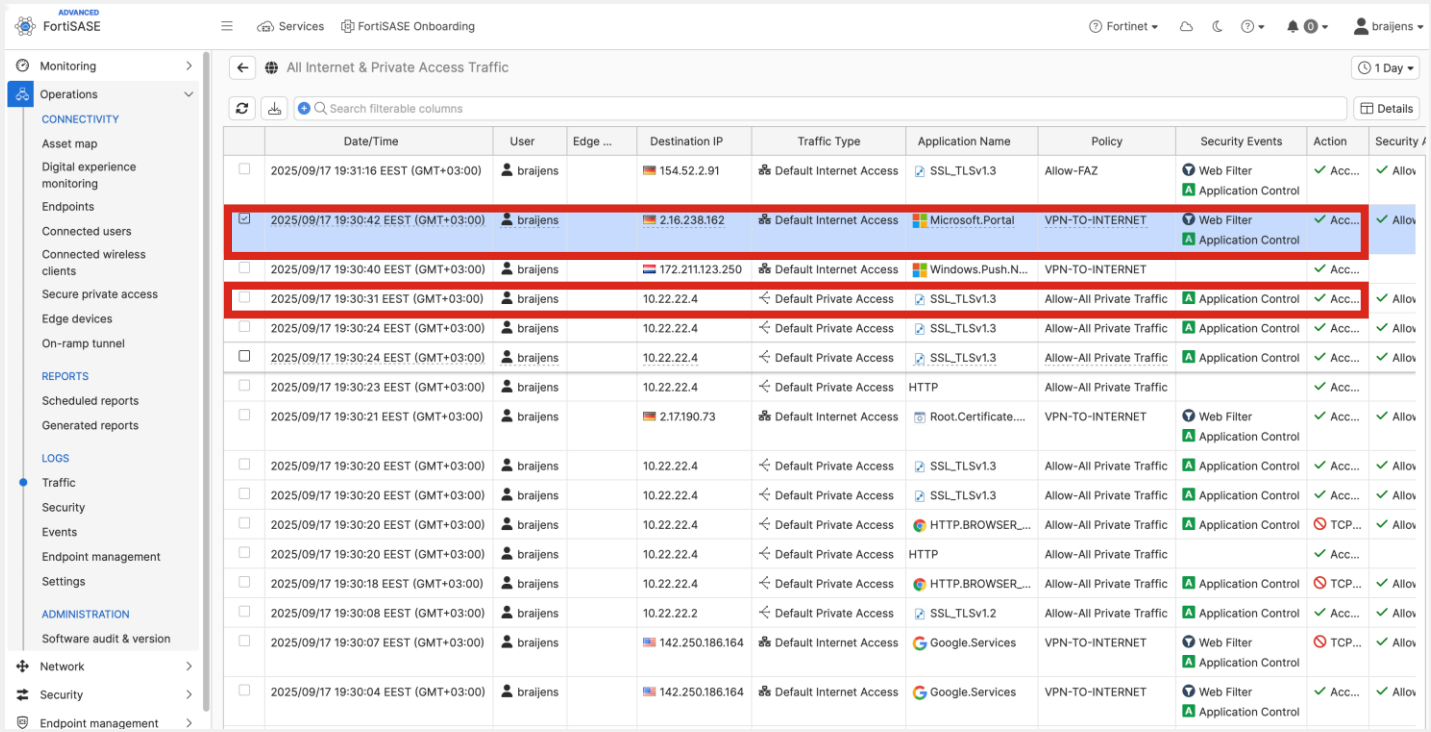


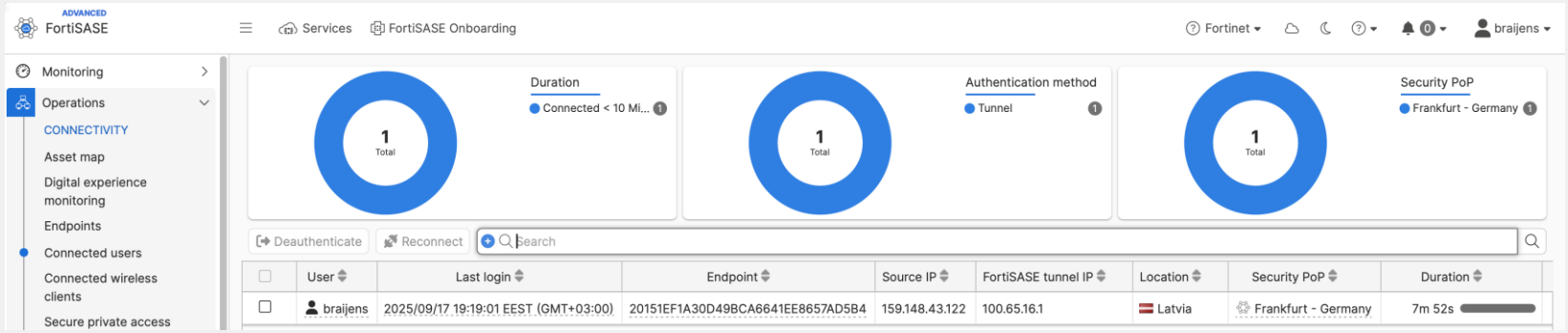
FortiSASE Agent (FortiClient)



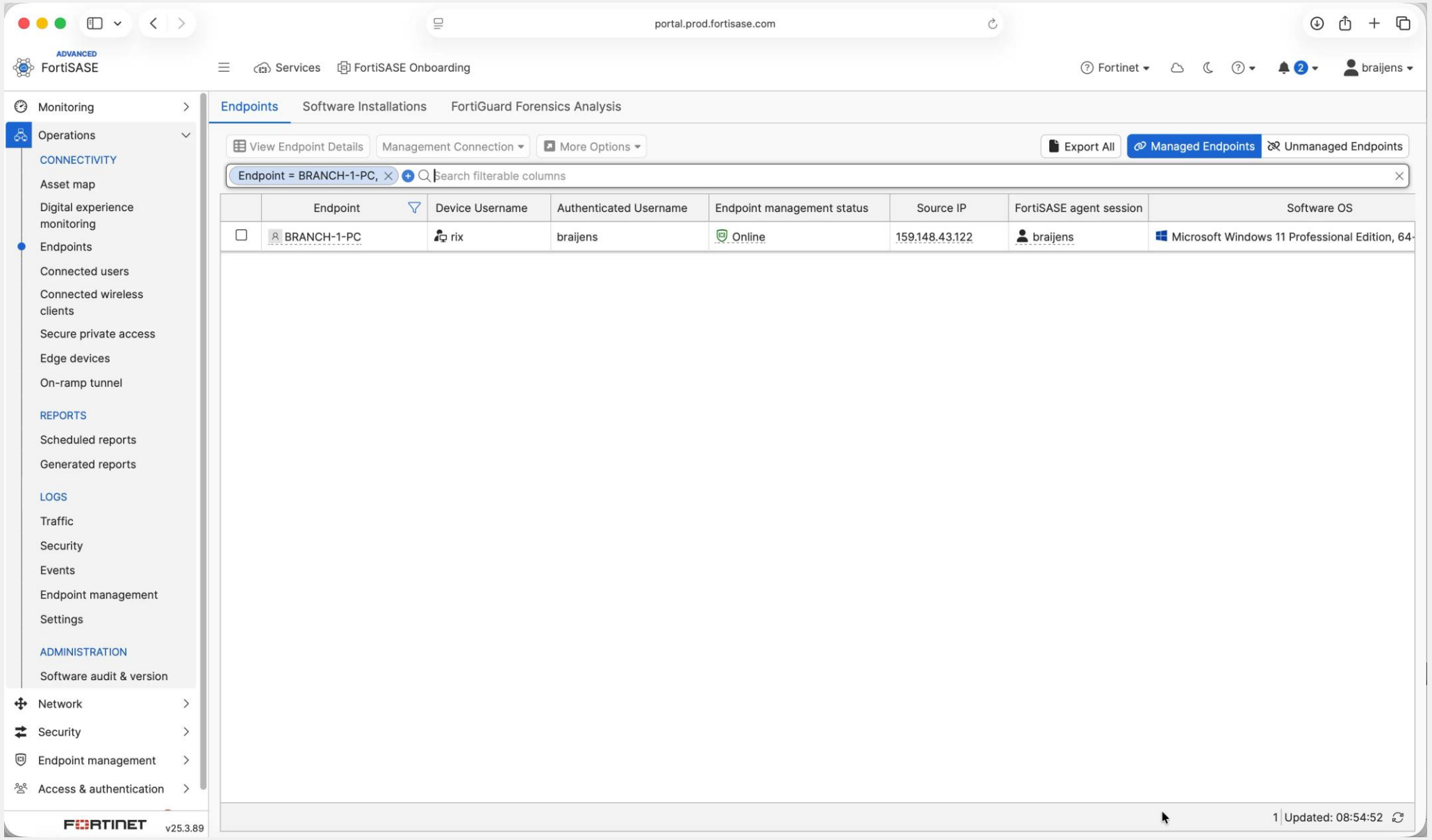
Agent (FortiClient)







Agent data on SASE portal



Secure Private Access

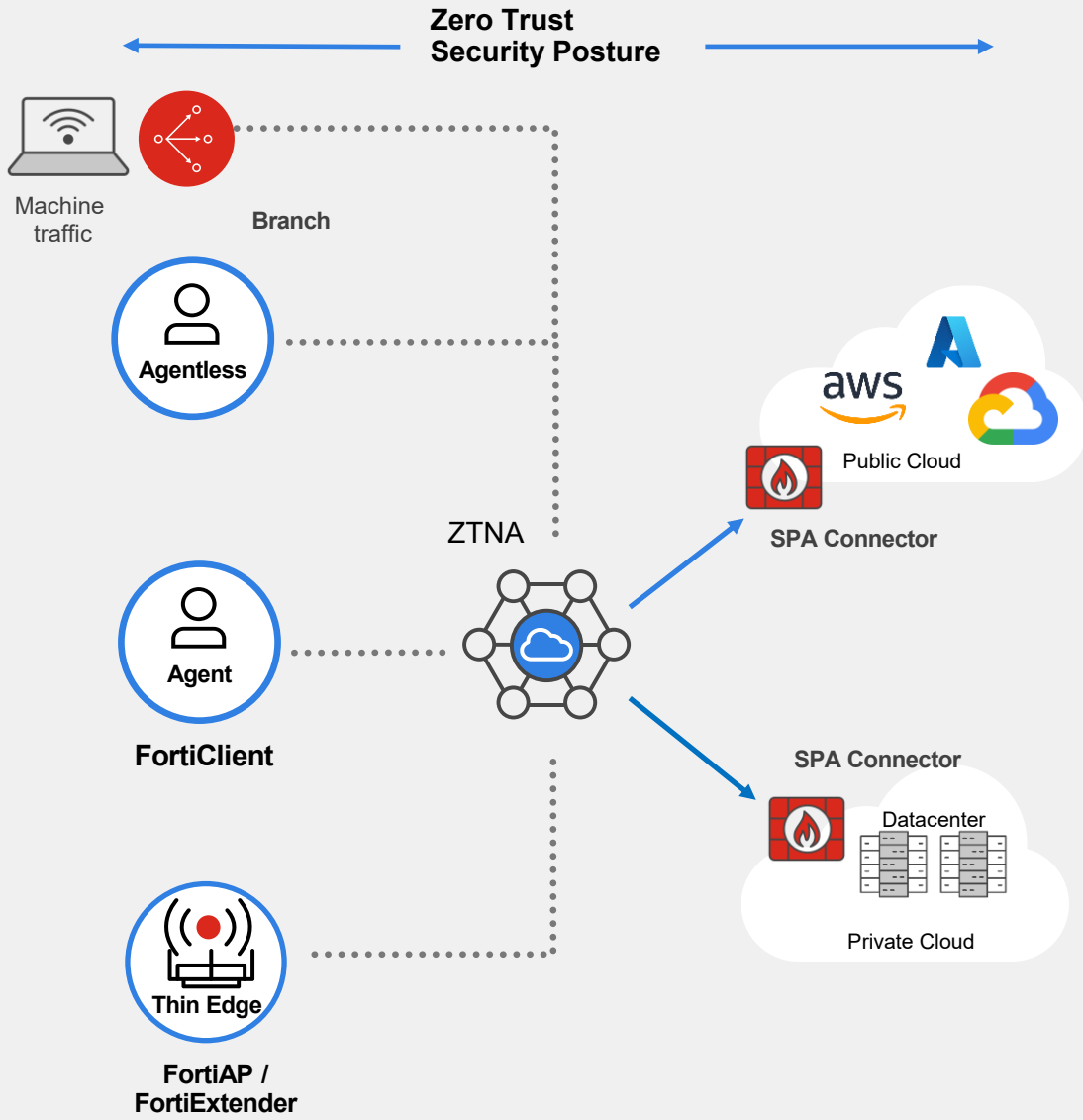
With ZTNA integration

Secure Cloud & datacenter app access

Secure anywhere access to corporate applications in datacenter and cloud with deep security inspection

Universal Zero-trust Network Access

User identity and device context-based zero-trust access to explicit applications from remote or on-prem location. Agentless flexibility via portal.



Secure SaaS Access

For Visibility and Control

Cloud App Access Control

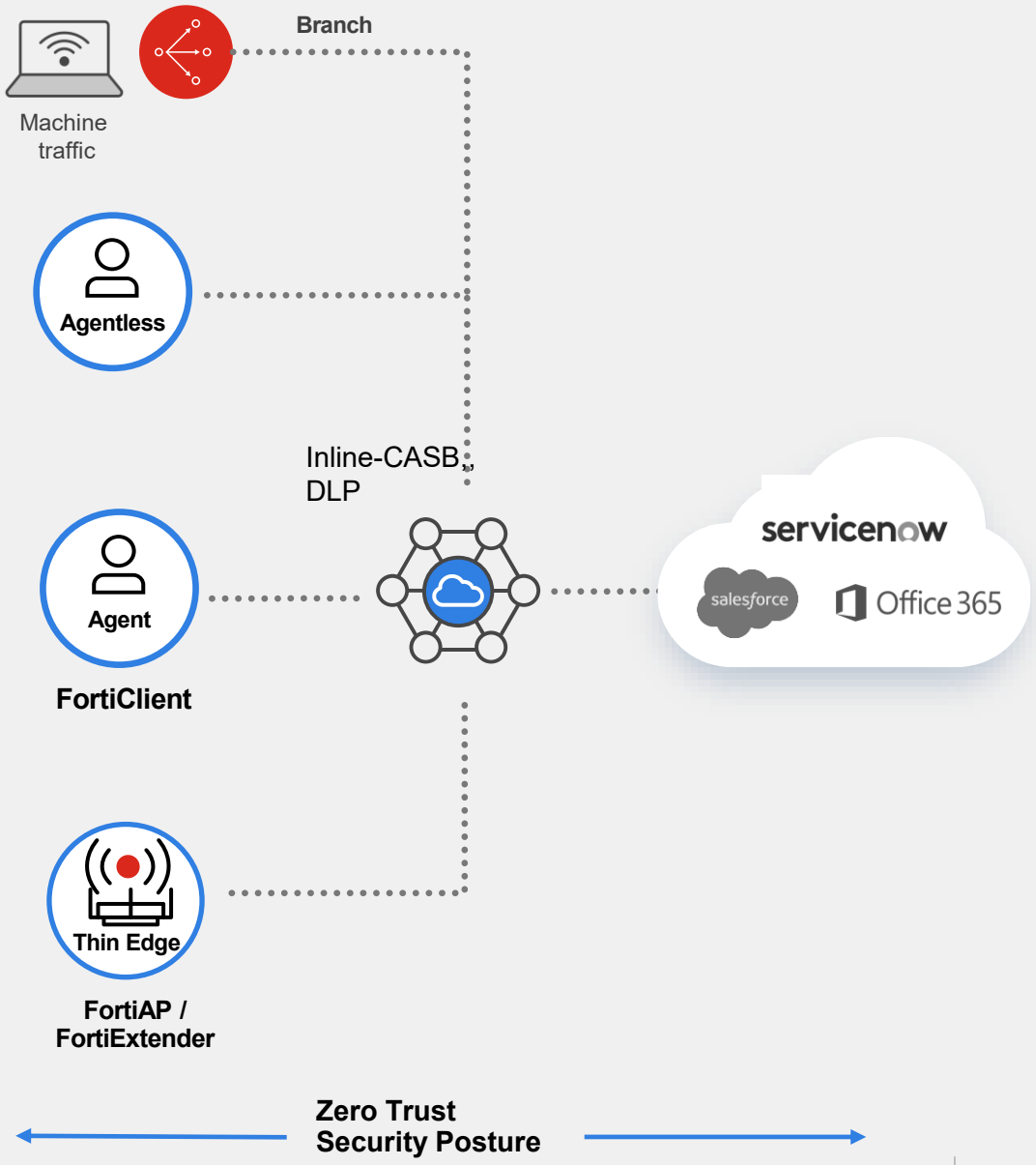
Safe Cloud Application access based on user context and blocking of malicious apps with in-line CASB feature, including Zero Trust posture checks

Deep control & view of apps content

Control over app content and files for enhanced security and threat detection

Unified agent for anywhere detection

FortiClient Agent covers all the use-cases from SASE, Zero-trust, SaaS security, and End-Point Protection



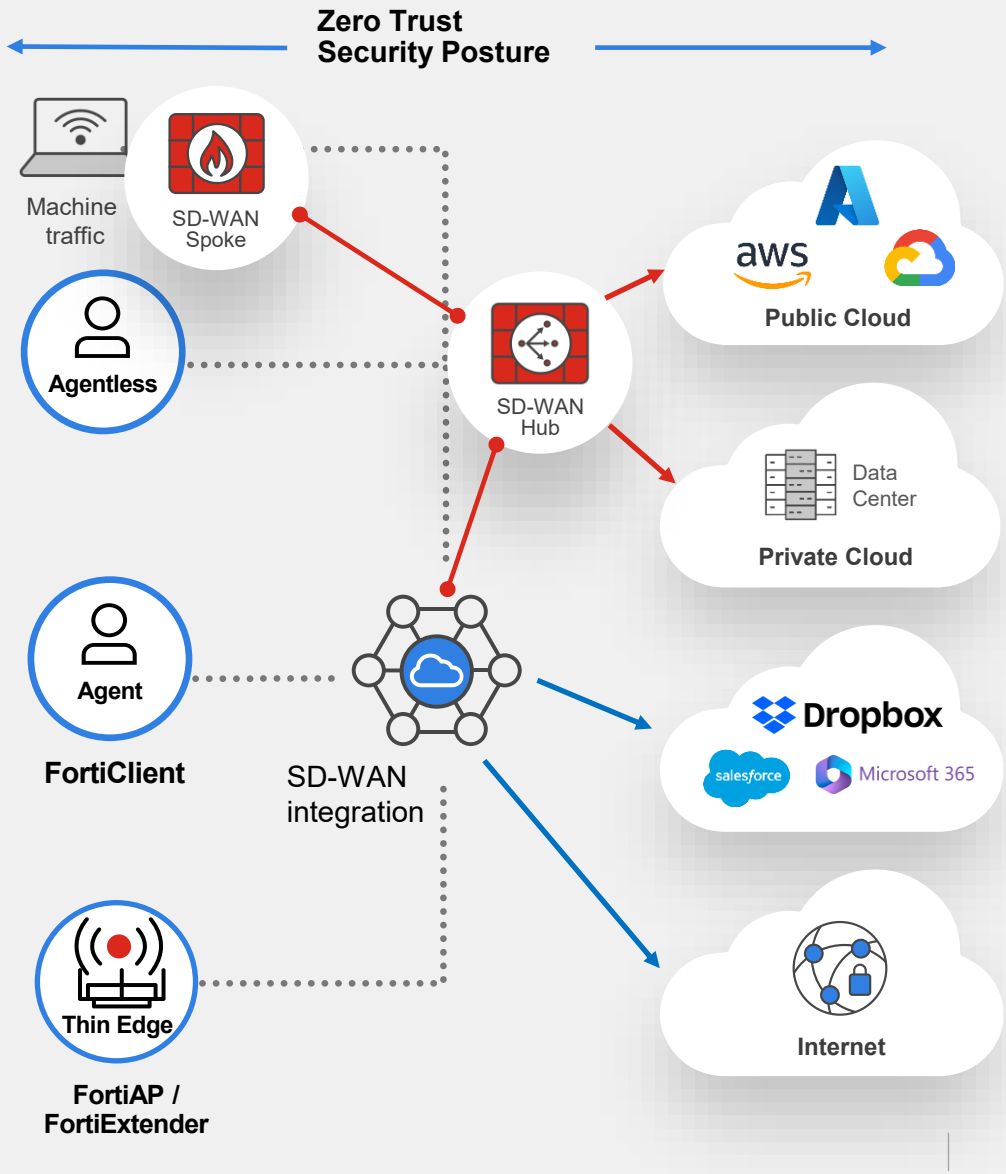
Secure Private Access with SD-WAN Integration in 5 min!

SD-WAN Private Access

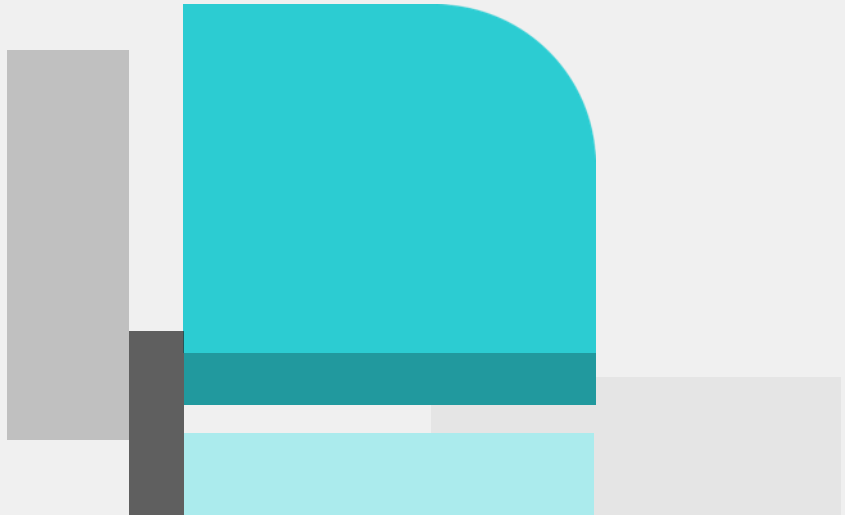
SD-WAN Integration with existing SD-WAN Hub from any **SASE PoP**

Fast access to applications using **SD-WAN** from SASE PoP to SD-WAN Hub

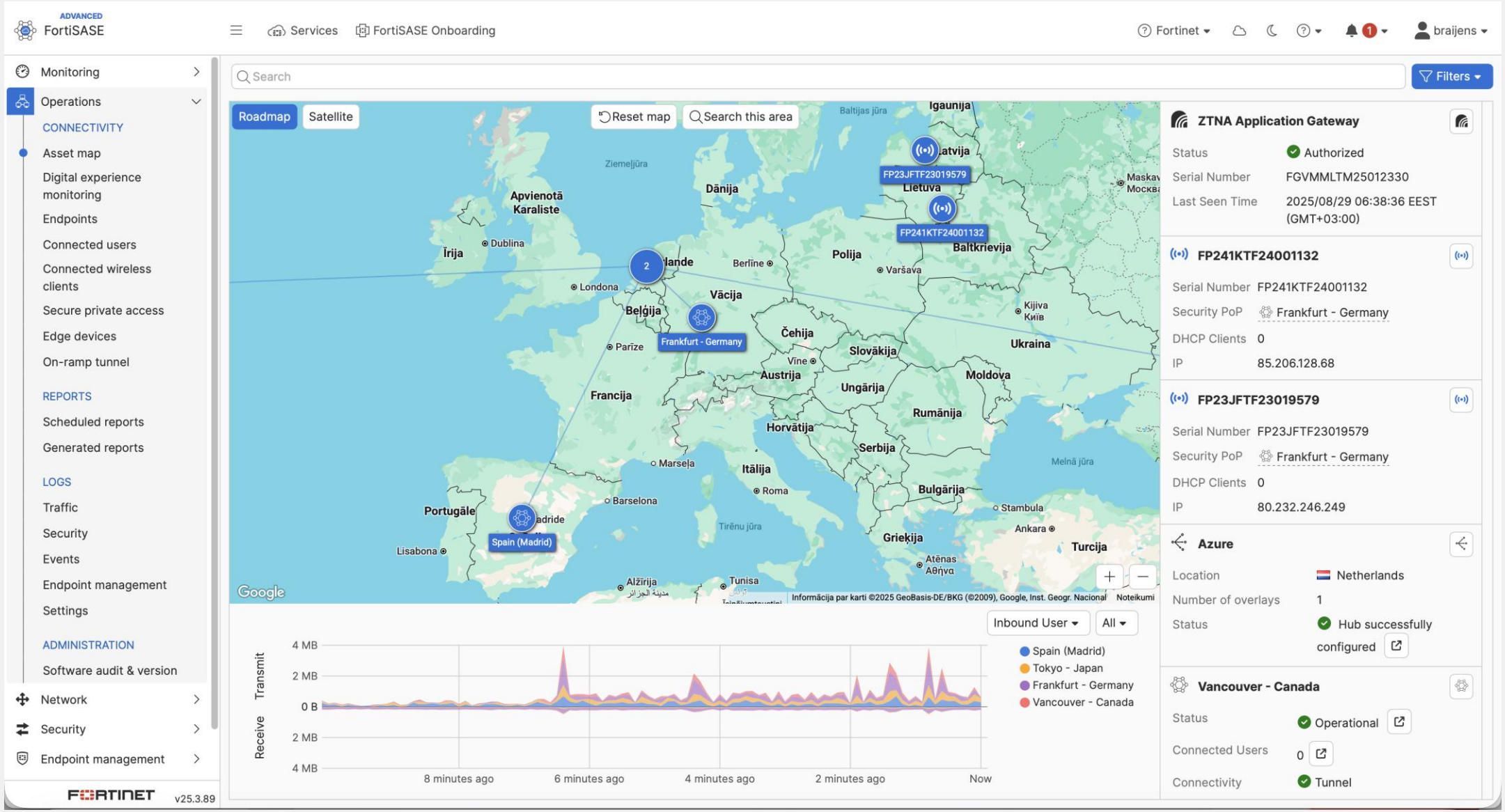
Broader app support
(UDP-based VoIP, video, UC)



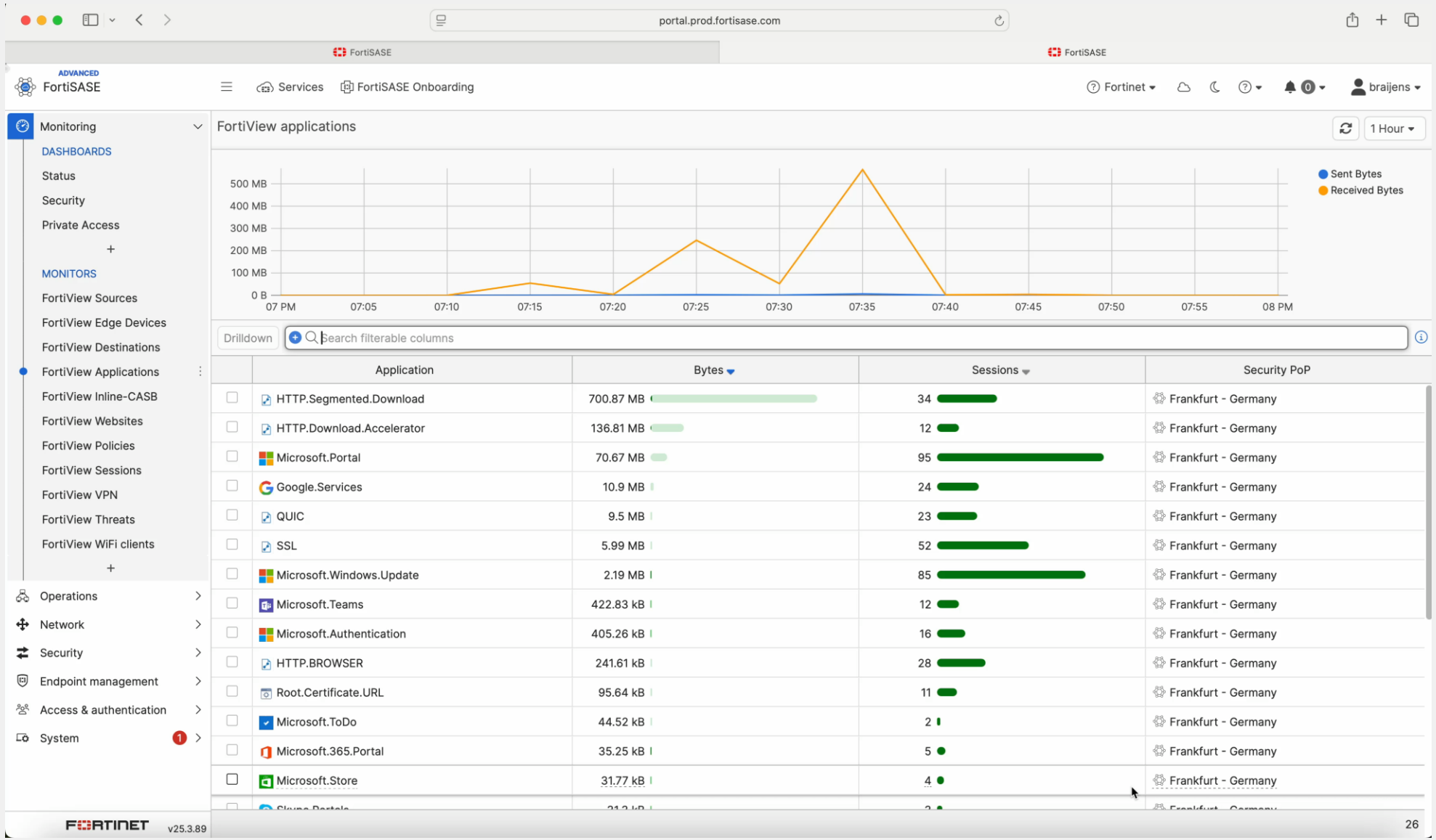
Visibility



Assets maps



FortiView



Thin Edge

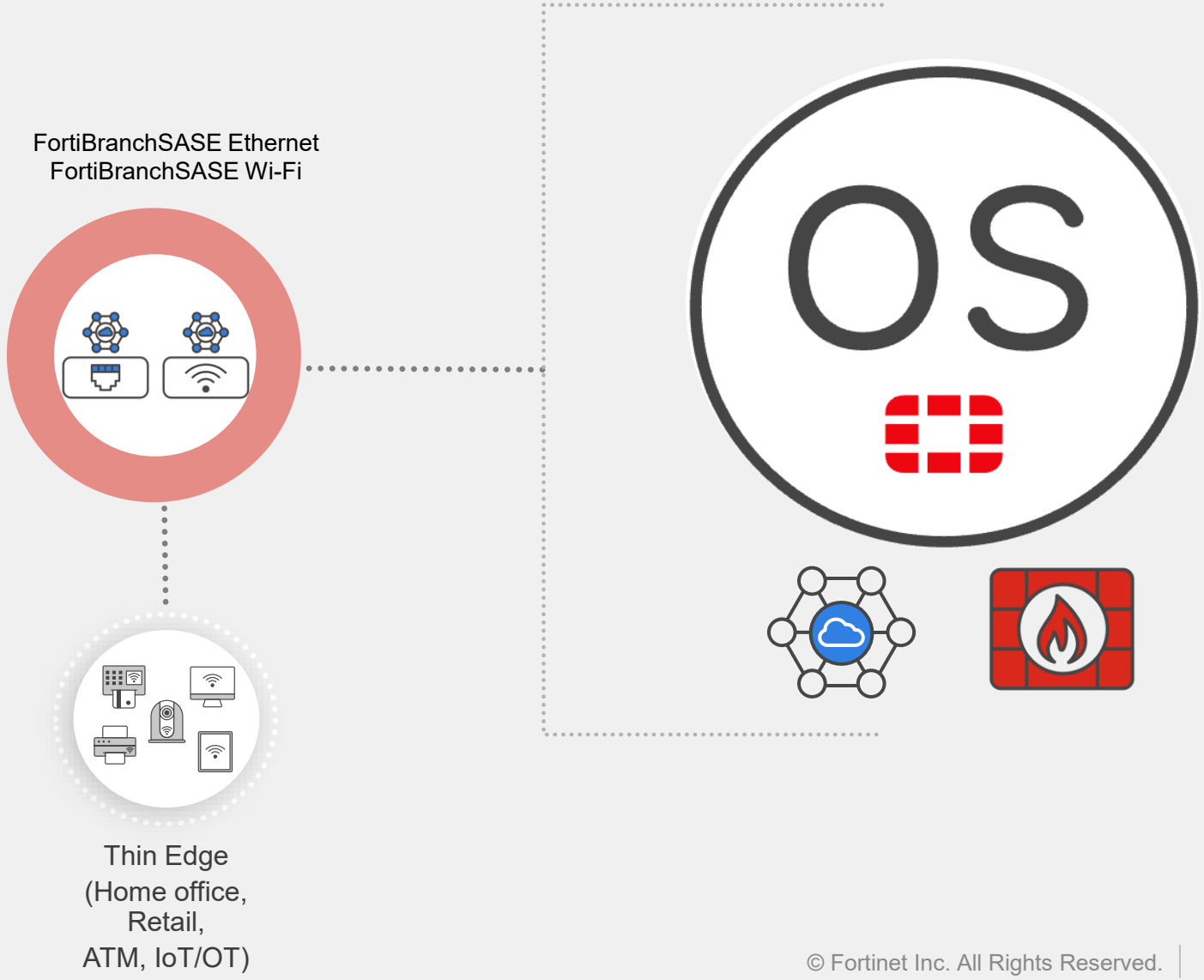
Flexible security for Thin Edge deployments

FortiBranchSASE

Secure Smaller Locations
Secure small locations, pop-up locations or home offices without the need of a firewall

IoT, OT and Agentless Devices
Secure access using built-in hardware agent for devices without any agents (e.g. IoT/OT, ATM)

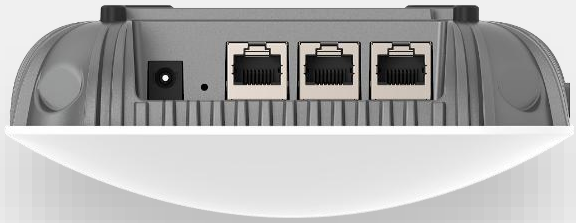
Central Visibility and Management
Unified management and visibility for all edges with deployment flexibility



FortiBranch SASE - More Models and More Devices

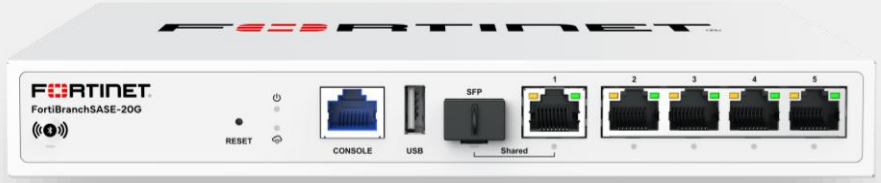
The Solution

- In 24.4.b the Maximum number of FortiExtender supported is 1024
- FortiSASE Support FortiBranch SASE models:
  - FortiBranchSASE-10F-WiFi
  - FortiBranchSASE-20G
  - FortiBranchSASE-20G-WiFi



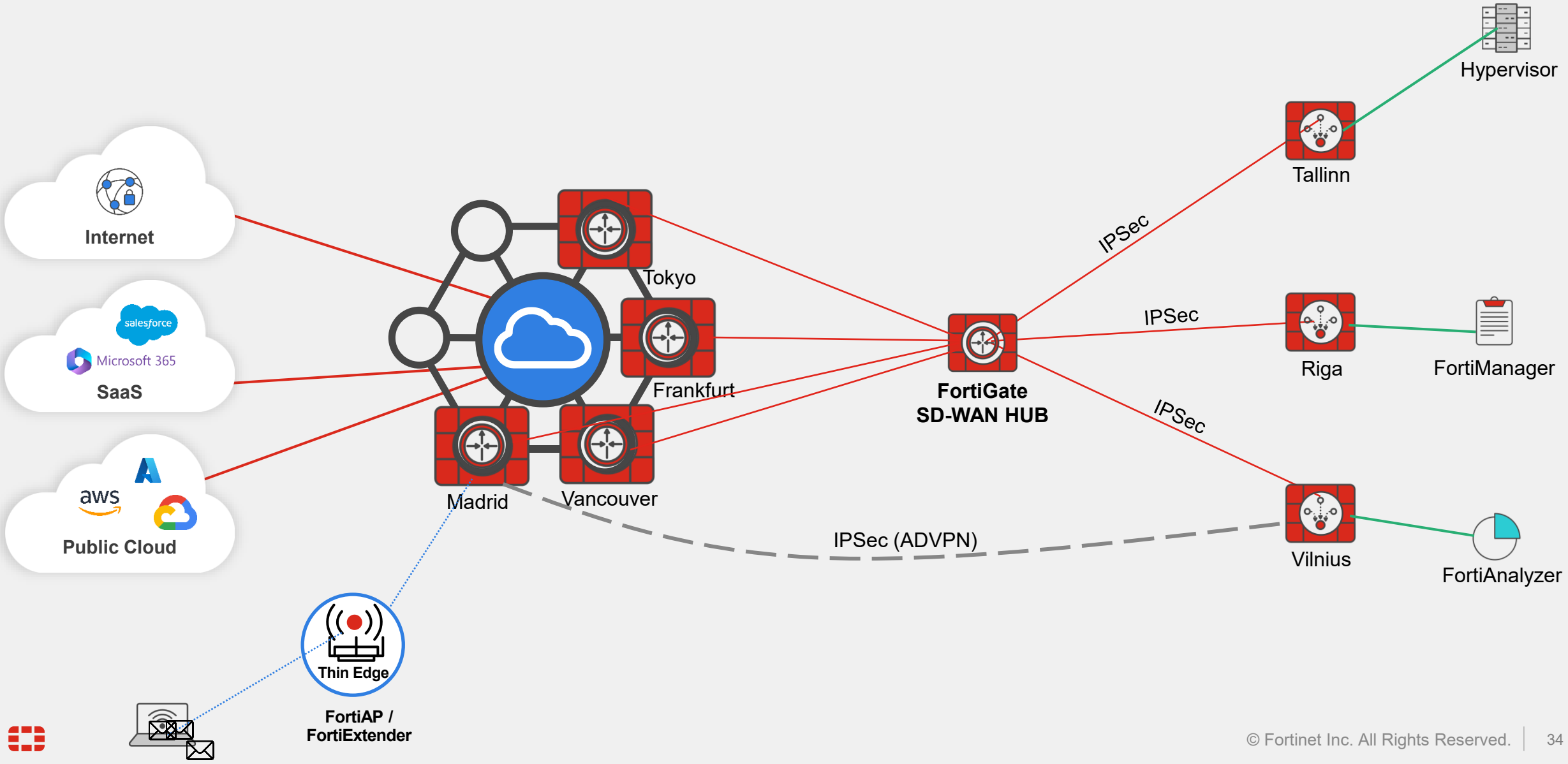
FortiBranchSASE 10F-WiFi

FortiBranchSASE 20G-WiFi

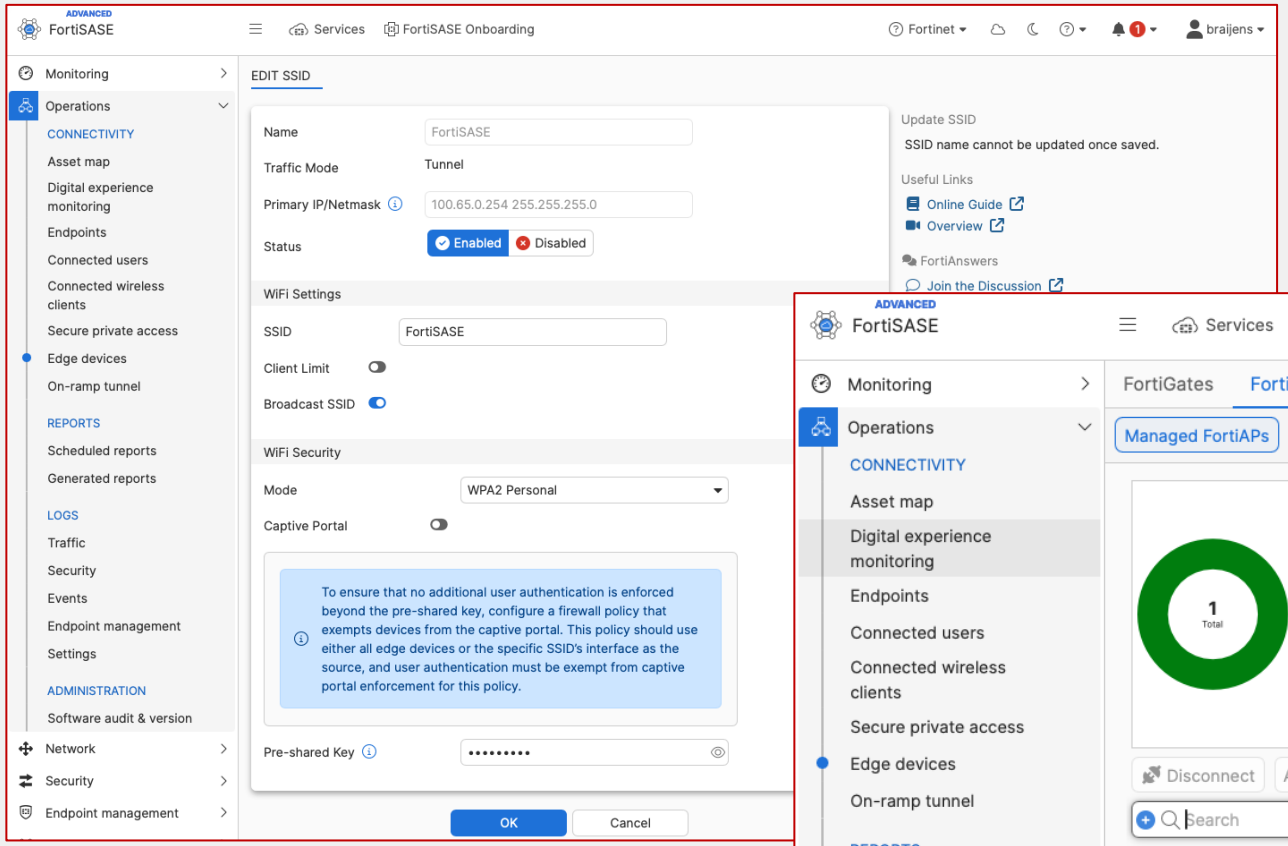


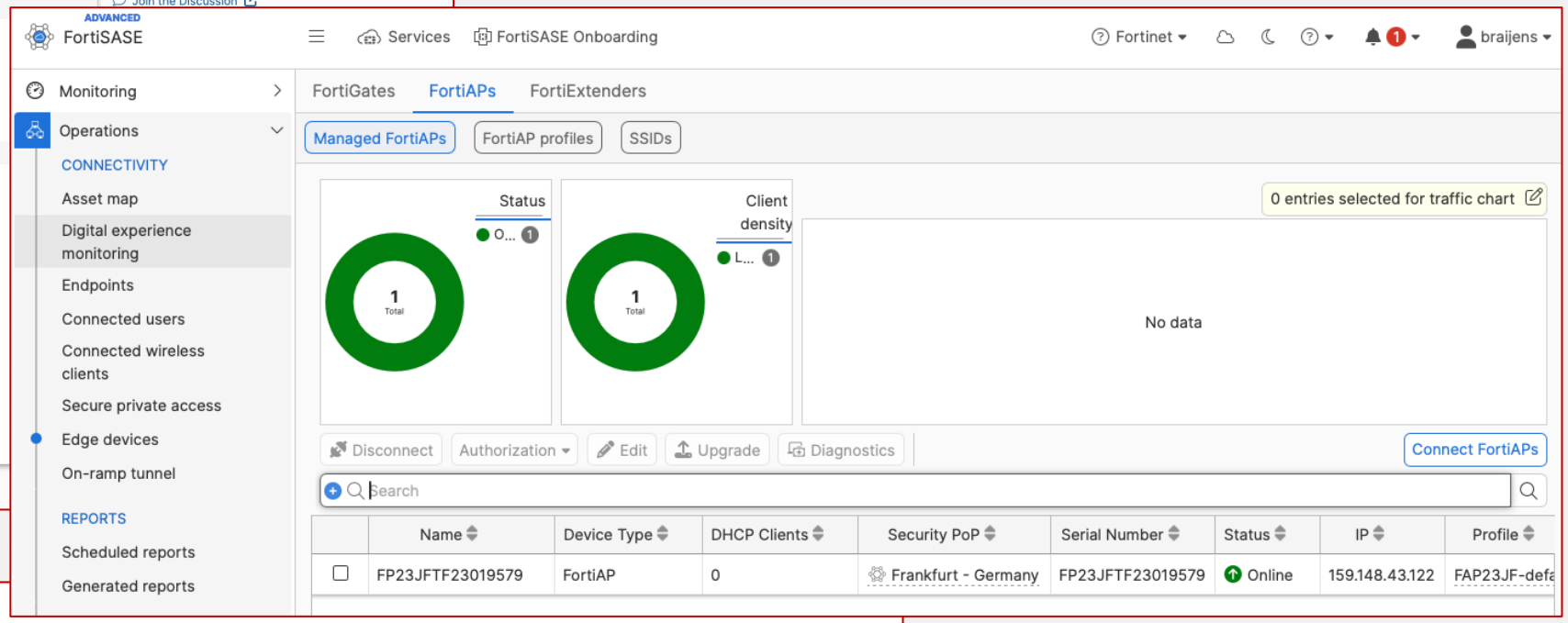
FortiBranchSASE 20G

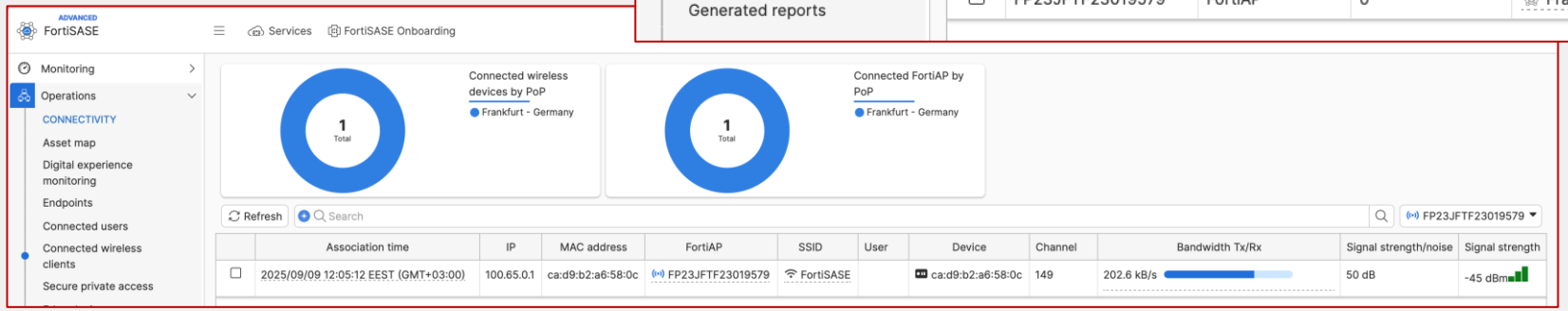
FortiSASE Thin Edge



FortiSASE ThinEdge







When to definitely consider SASE?

- Majority of users are working elsewhere and you want to implement same level of security as in office
  - HQ becomes Single Point of Failure
  - cost - double (or even triple) internet pipe bandwidth + correctly sized FortiGate (with necessary subscriptio
- Most of your services are not on-prem (SaaS, Public Cloud, even DC)
  - No point in hauling data to central location instead of connecting directly
- Lots of small shops/branches
  - single pane of management for users and sites alike

When you don’t need to consider SASE?

Always consider SASE ☺

- if you have necessary puzzle pieces, build your own solution with relevant use case from SASE
- if Excel is against you, go for partially or fully for SASE (and leverage existing knowledge/install base)

Thank You!