On Demand Replay: https://register.gotowebinar.com/recording/4244933349224122116

FORTINET®

SASE As Easy as 1-2-3

Feb 23, 2023

Nirav Shah, Alexandra Mehat, Sarbjeet Singh

Agenda

01 Define: SASE, SSE, Single Vendor SASE

02 Evolving Vendor Landscape

03 Fortinet SASE Solution

04 Simplified Licensing

05 Record Win Rate and Deal-Flows

06 Objection Handling

07 Go To Market and Competitive Info

Step 1 : Why and What is SASE ?

All about terminology and vendor landscape

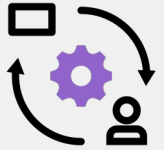
Customers Strategic Focus Areas

Working From Anywhere is the new workplace

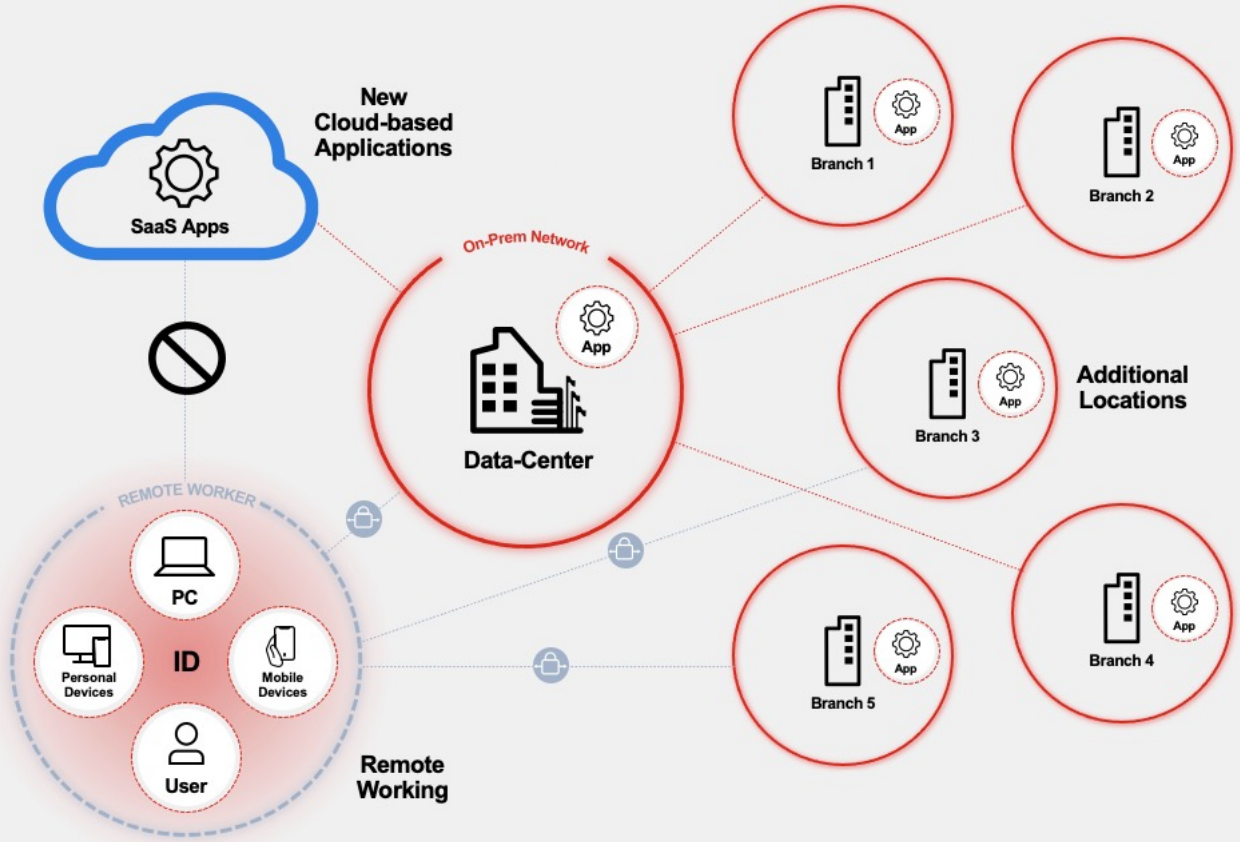
Cloud and SaaS are the new application stack

Direct Internet is the new connected network

Zero Trust Mindset is the focus area for access



Challenges with Existing Network



- **Struggle to Secure Remote Workers**
- **Lack of Higher User Experience**
- **Complex and Lack of Visibility**
- **Lack of Staff to Maintain Network**

What is SASE ?

As defined by Gartner – SASE stands for Secure Access Services Edge

Gartner®

SASE converges on-prem networking and cloud-delivered security to enable secure access to applications for remote users and thin branch offices

What is SSE ?

As defined by Gartner – SSE stands for Secure Services Edge

Secure ~~Access~~ Services Edge

SSE is a component of SASE to provide cloud-delivered security and hosted by vendors. It is often OpEx (Per User Per Year) based pricing.

SASE – Two Primary Pillars

Networking and Cloud-Delivered Security (SSE)

SD-WAN - Software Defined WAN
Determine the most effective way to route application traffic between branch offices & DC

SWG - Secure Web Gateway
Enforce safe browsing habits at the endpoint (eg. URL filtering, DNS filtering, SSL inspection)

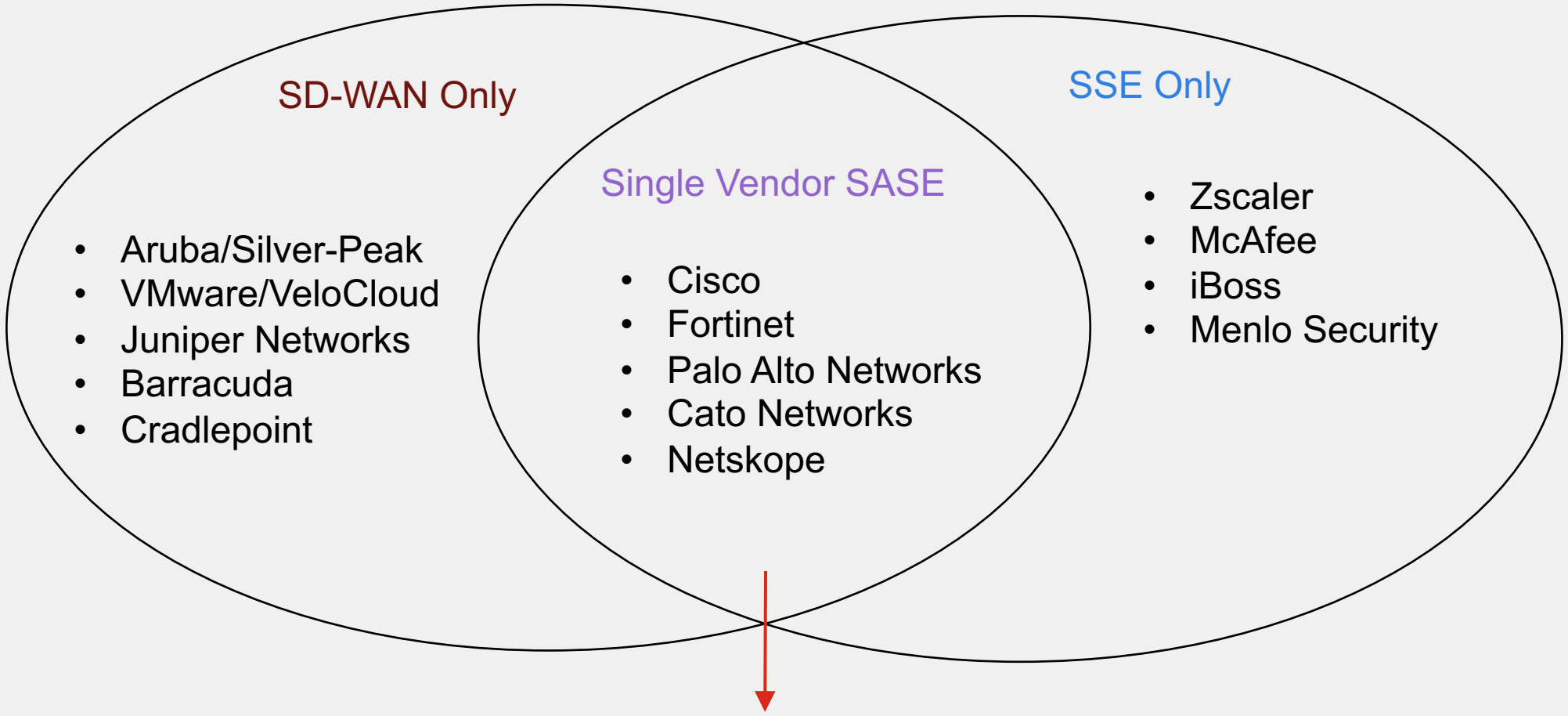
CASB - Cloud Access Security Broker
Control and monitor access to SaaS applications

ZTNA - Zero Trust Network Access
Verifies the user identity, context and policy when accessing applications.

DLP - Data Loss Prevention
Monitors outbound network traffic for unauthorized sensitive data exfiltration (eg. credit card nb)

Single Vendor SASE	
SD-WAN	SSE
• On-prem device • WAN Edge • Routing • Quality of Service	• Cloud-delivered • SWG • FWaaS • ZTNA • CASB • DLP

Vendor Landscape : SD-WAN, SSE and SASE



Consolidation, Consistent Security, Lower Cost

Gartner Magic Quadrant and Market Guide for SASE

2022 Gartner SD-WAN MQ

FORTINET®

Market Guide for Single Vendor SASE

Market Guide for Single-Vendor SASE

Published 28 September 2022 - ID G00768660 - 25 min read

By Analyst(s): Neil MacDonald, John Watts, Jonathan Forest, Andrew Lerner

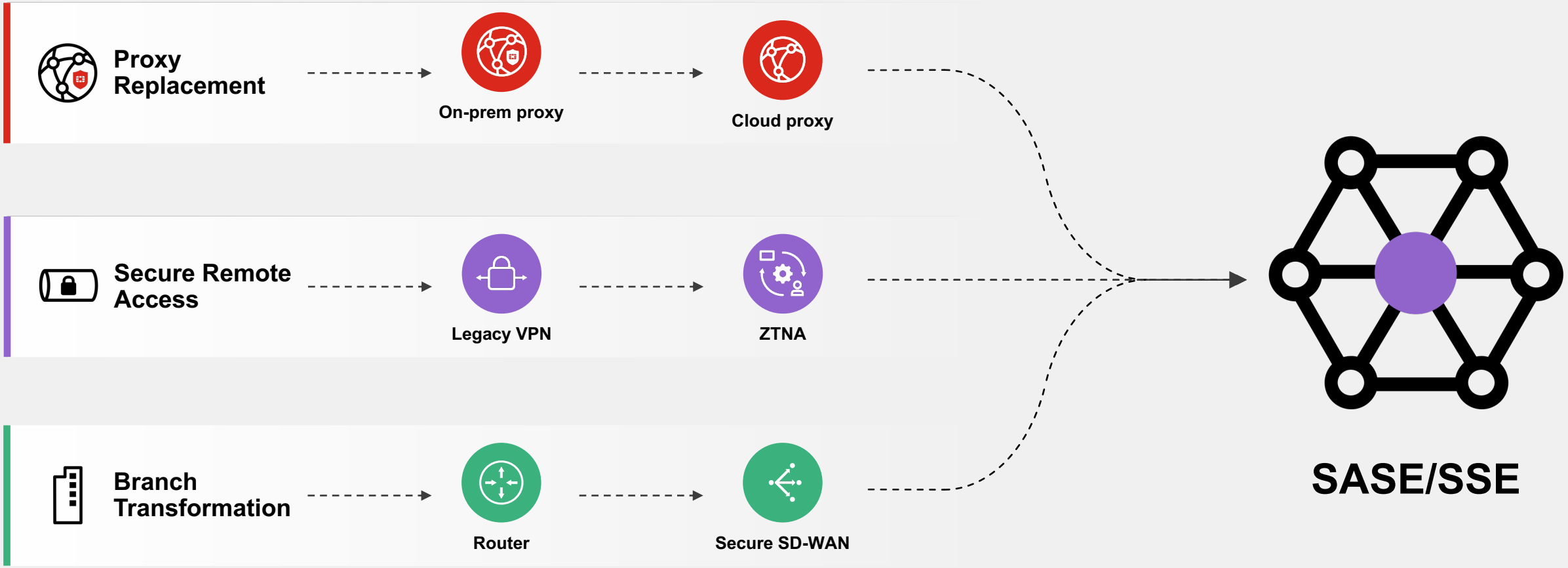
Initiatives: Cloud and Edge Infrastructure; Infrastructure Security

> Single-vendor SASE delivers converged network and security capabilities to connect and secure distributed users, devices and locations to resources in the cloud, edge and on-premises. Infrastructure and operations leaders should use this research to analyze the emerging single-vendor SASE market.

FORTINET®

2022 Gartner SSE MQ

Discovery - Customer Initiatives for SASE and SSE



Poll 1

Which SASE Strategy Preferred by your Customers (Pick One)

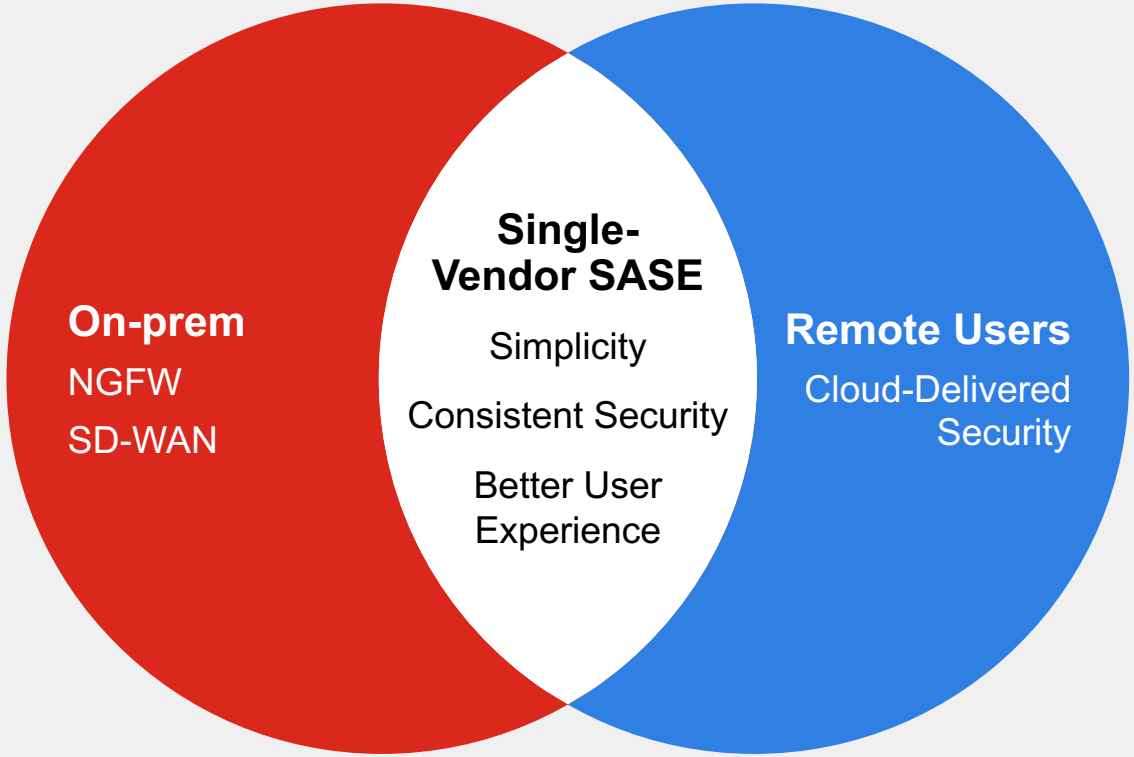
- SSE
- SASE with Dual Vendors
- SASE with Single Vendor
- None

Percentage of your customer accounts

Step 2 : Introduce Fortinet SASE

How is it solving customer problems in unique way ?

Fortinet’s Strategy for Single Vendor SASE Provider



Three Key Components

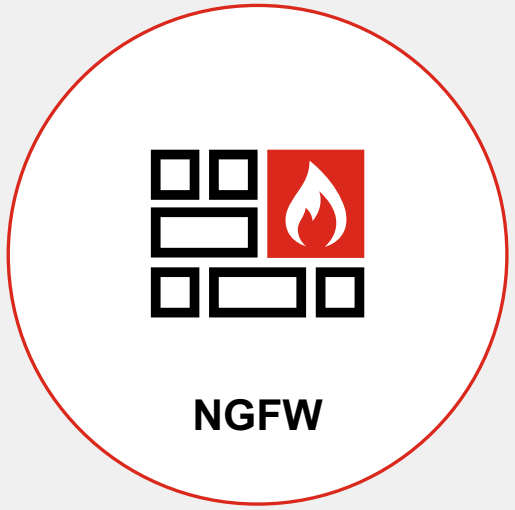
- **FortiOS Powered Convergence**
- **AI/ML Driven FortiGuard Security**
- **Unified FortiClient Agent**

Pragmatic Journey to SASE

With Fortinet's convergence of security and networking everywhere

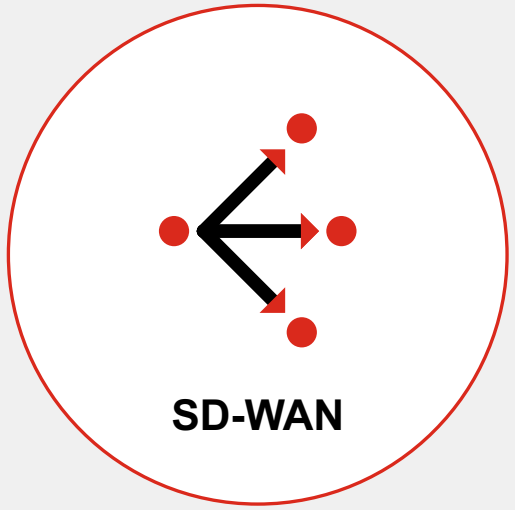
1

Secure Edge Connectivity



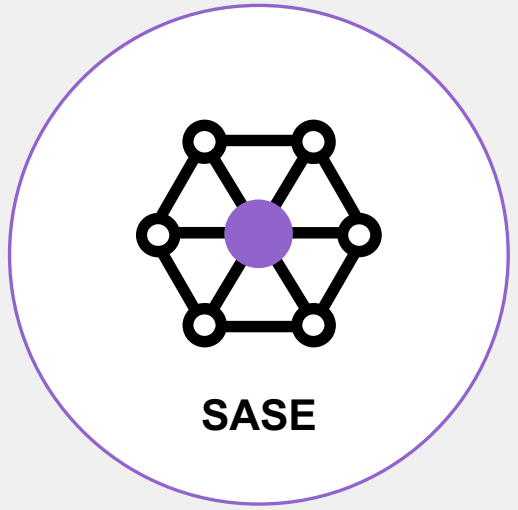
2

Optimize Application Experience



3

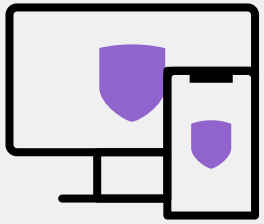
Secure Remote Users



FortiSASE – Cloud Delivered Convergence

Cloud-delivered security with Integration with On-Prem Networking

Securing Remote Users

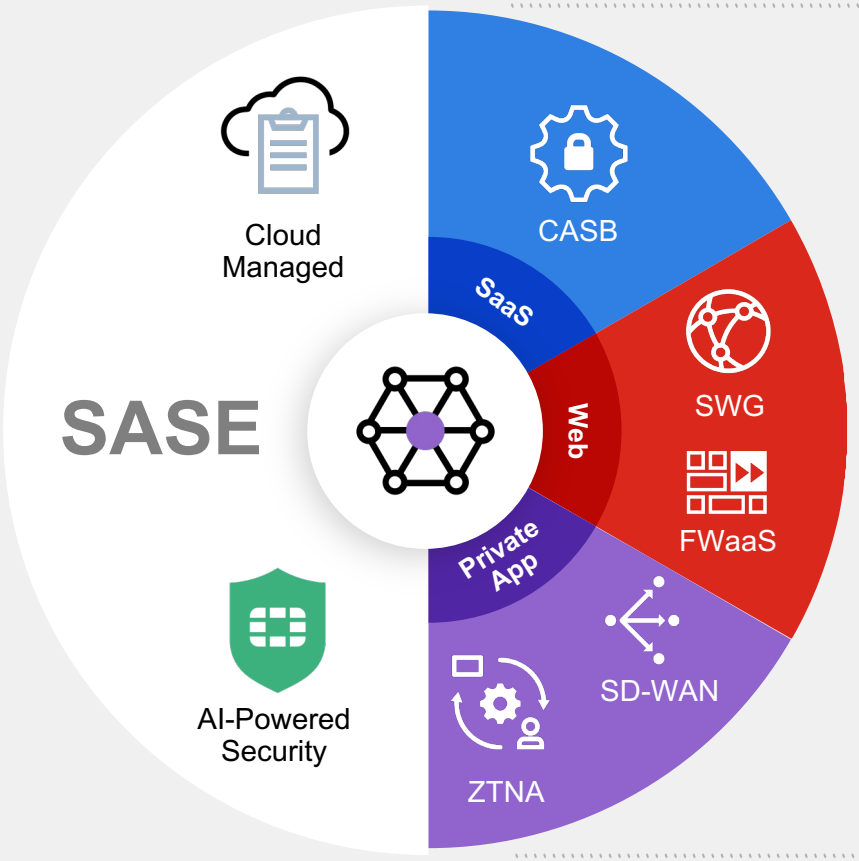


FortiClient Unified Agent

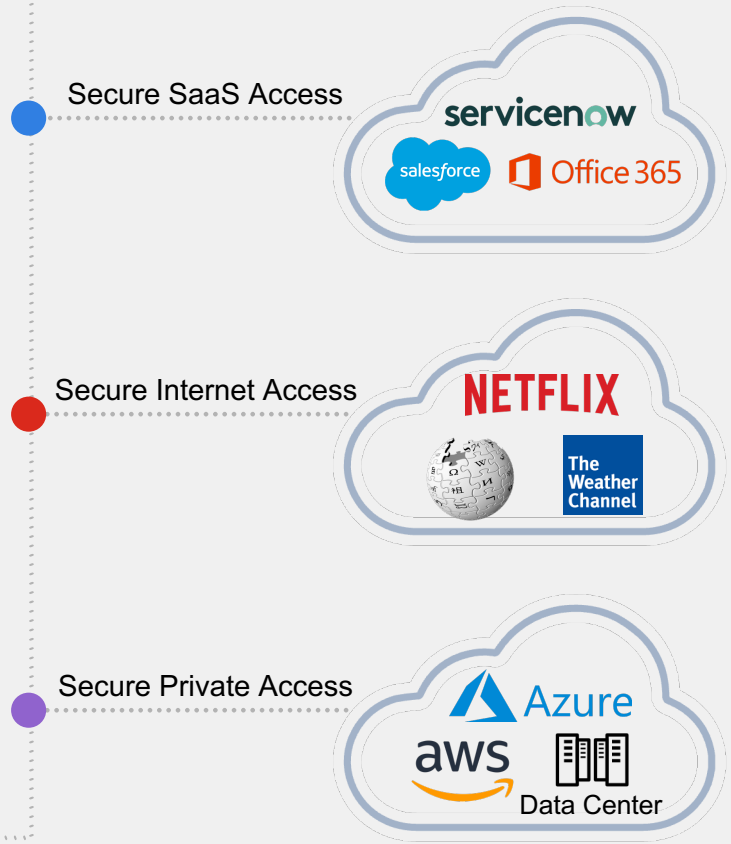
Securing Thin Edges

FortiExtender

Cloud-delivered Security & Networking



Improved User Experience



FortiSASE Point of Presence Investment

- Several New PoP are added in last 12 months
- Follow NFR process and work with CSE team

- Recently Added
  - Miami
  - Dubai

- Coming up
  - San Paolo, Brazil

- Noteworthy in planning based on NFR
  - India
  - Hong Kong
  - Turkey
  - South Africa

Simple User based Licensing for Remote Users

SASE Offering SKU

Simple Turnkey Offering for Single-vendor SASE Solution

FWaaS & SWG: L3-7 Firewalling, URL-Filtering, Anti-Malware, DNS Filtering

ZTNA : Cloud-Provisioned, Device Posture checking, Continuous assessment

CASB : In-line CASB and API-Based for Managed and unmanaged devices

Endpoint Security : EPP, Sandboxing, Vulnerability Management

Cloud Logging

Cloud Managed

24 x 7 Support

Supports 3 devices per user

[Link to Ordering Guide]

ORDER INFORMATION

REMOTE USERS	BANDS	FORTITRUST USER LICENSE
FortiSASE Remote	100-499	FC2-10-EMS05-547-02-DD
	500-1,999	FC3-10-EMS05-547-02-DD
	2,000-9,999	FC4-10-EMS05-547-02-DD
	10,000+	FC5-10-EMS05-547-02-DD

FortiSASE DEMO AS EASY AS 1-2-3

1 – Cloud based Management

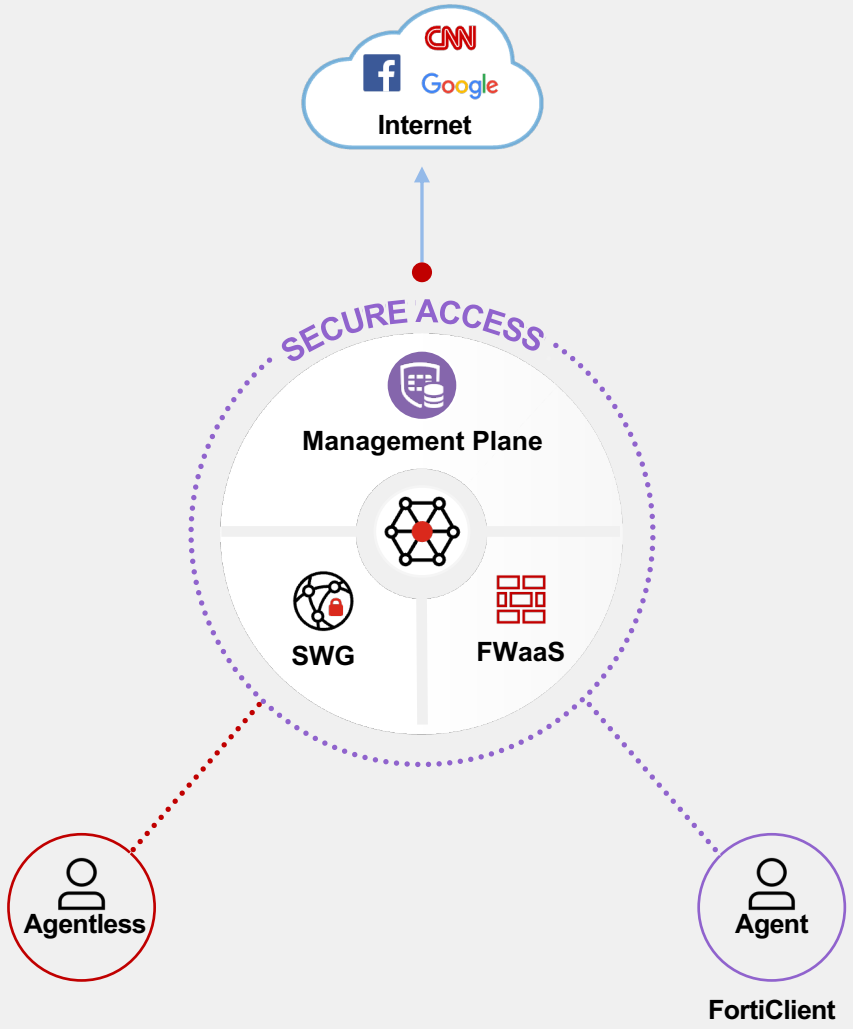
2 – Analytics and Visibility

3 – On-boarding users

USE CASE 1

Secure Internet Access for Remote Users

Surfing the Web safely



Safe browsing from anywhere

Malware & ransomware prevention

Continuously assess the risks and automatically respond to **counter known and unknown threats**

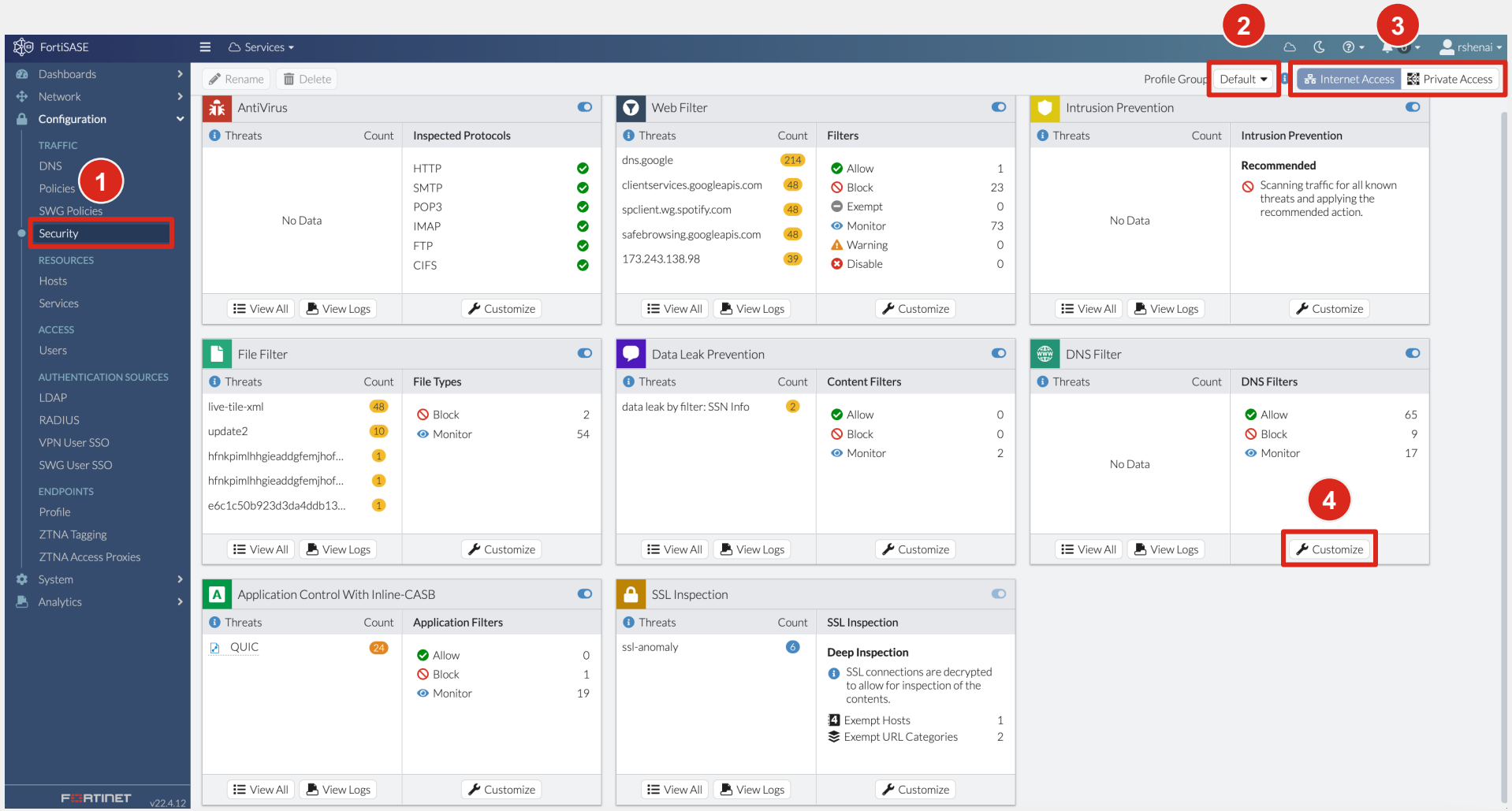
Deep inspection of end-user activity

Constant inspection of web activity for threats, even when using secured HTTPS access

Market Leading Security as a Service

Fortinet best-in-class Cloud security efficacy powered by FortiGuard Labs

Security Configuration—One Enforcement Location

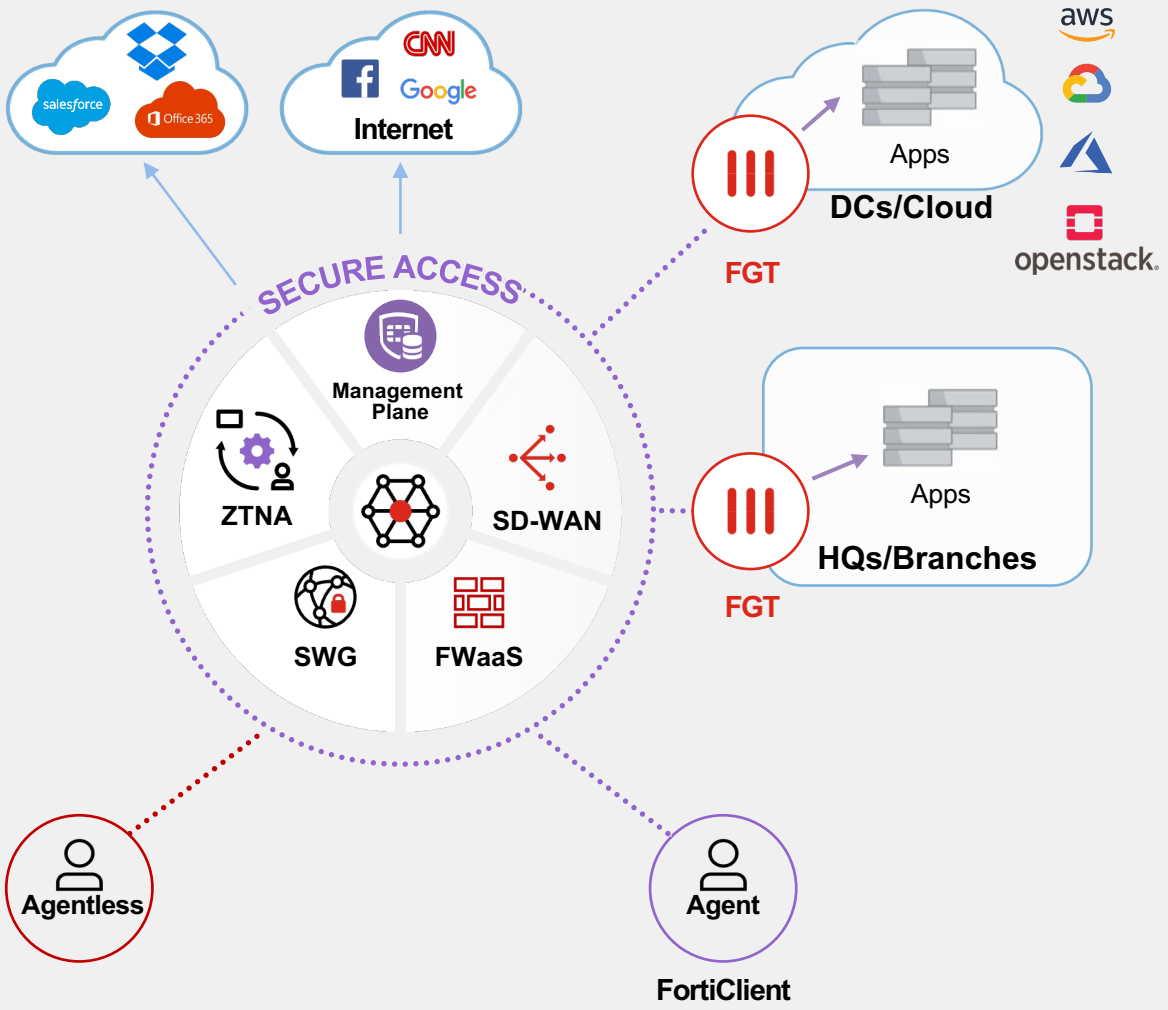


1. Simplified FOS Security from single pane
2. Default profiles available for fast consumption
3. Web and Private App visibility
4. Security profiles can be customized

USE CASE 2

Flexible Secure Access to corporate applications

Getting to the corporate applications safely



Secure corporate app access

Secure Cloud & datacenter app access

Anywhere secure access to corporate apps for asset protection and compliance

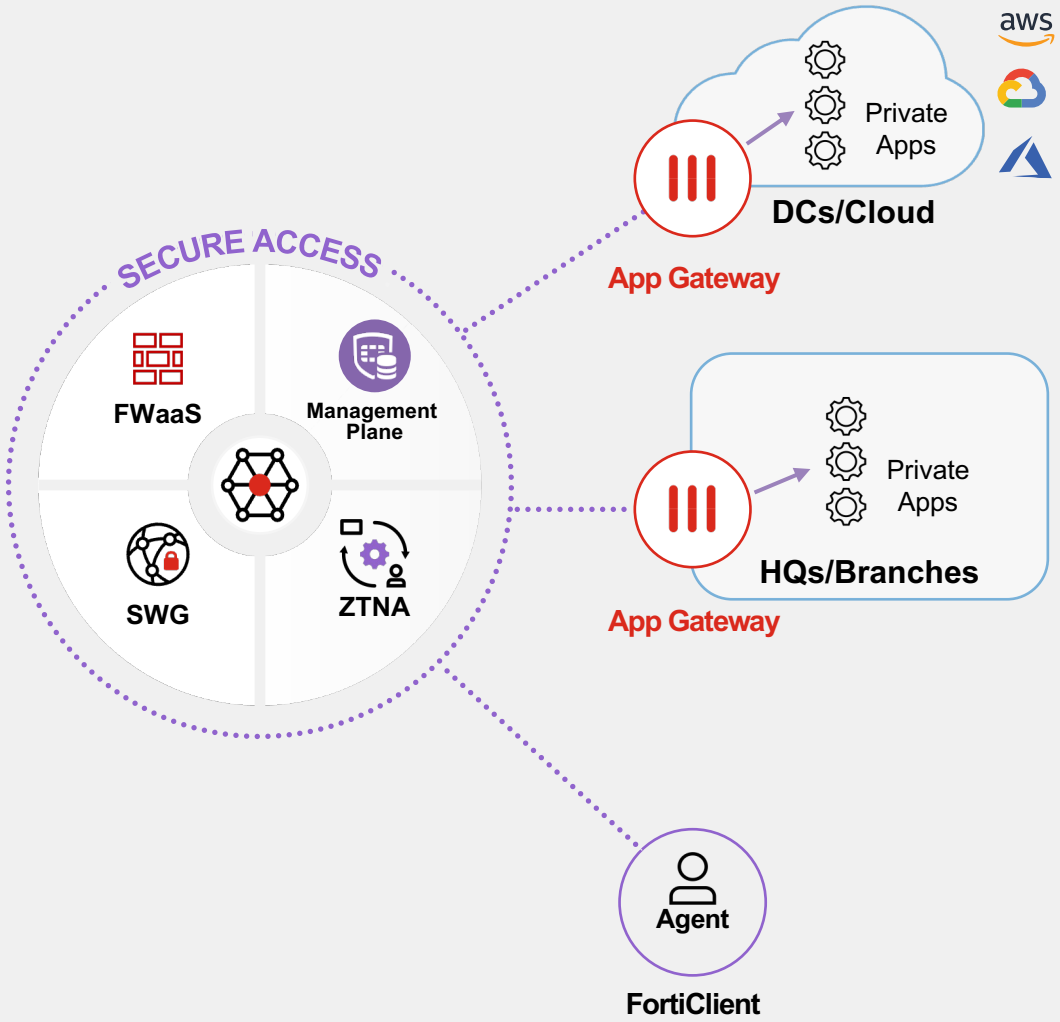
Highly granular Access Control

Context-based zero-trust access enforcement, app based and adaptive with AI/ML

On-prem SD-WAN integration

Superior user experience with full integration with Fortinet SD-WAN architecture

Secure Private Access With Natively Integrated ZTNA



Enabling Universal ZTNA

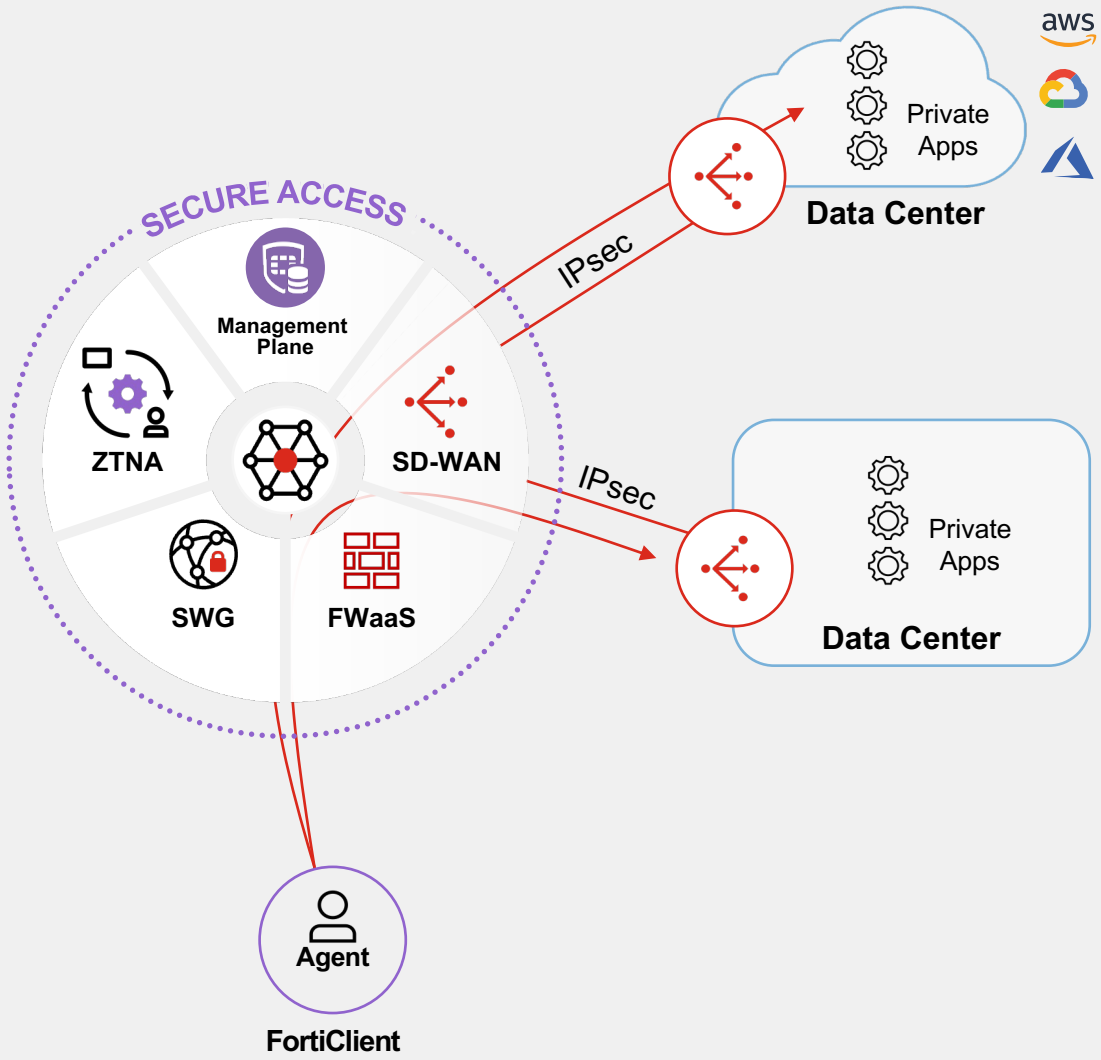
Cloud provisioned ZTNA connections

Device attributes, **user** info, **posture-based** security

Granular per-session posture checks

Continuous posture re-assessment

Cloud-delivered SD-WAN Integration With SSE

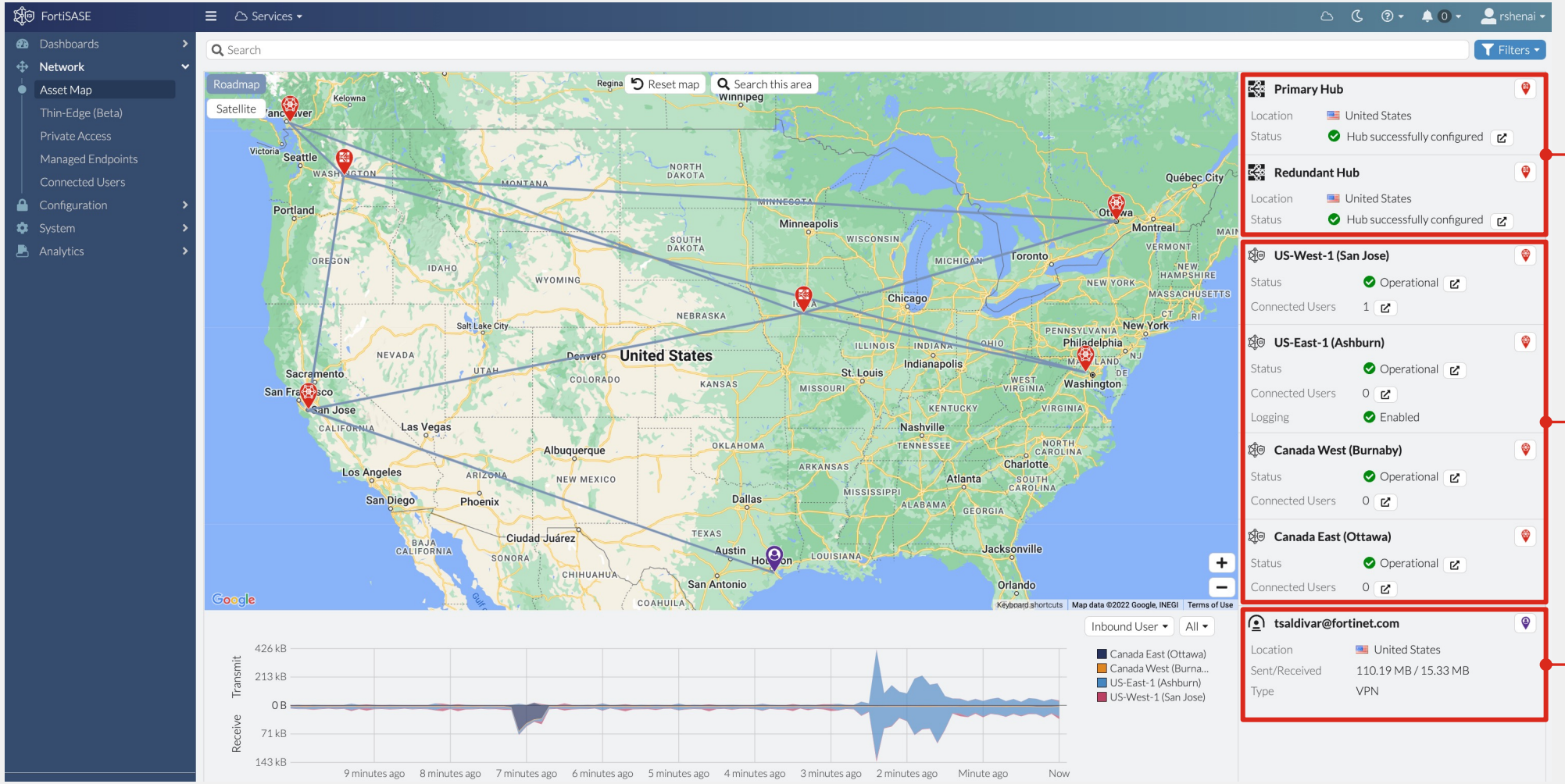


SD-WAN Private Access

- Augment to existing **SD-WAN**
- **Intelligent** routing & steering
- **Broader app support** (UDP-based VoIP, video, UC)

FortiSASE Secure Private Access with SD-WAN

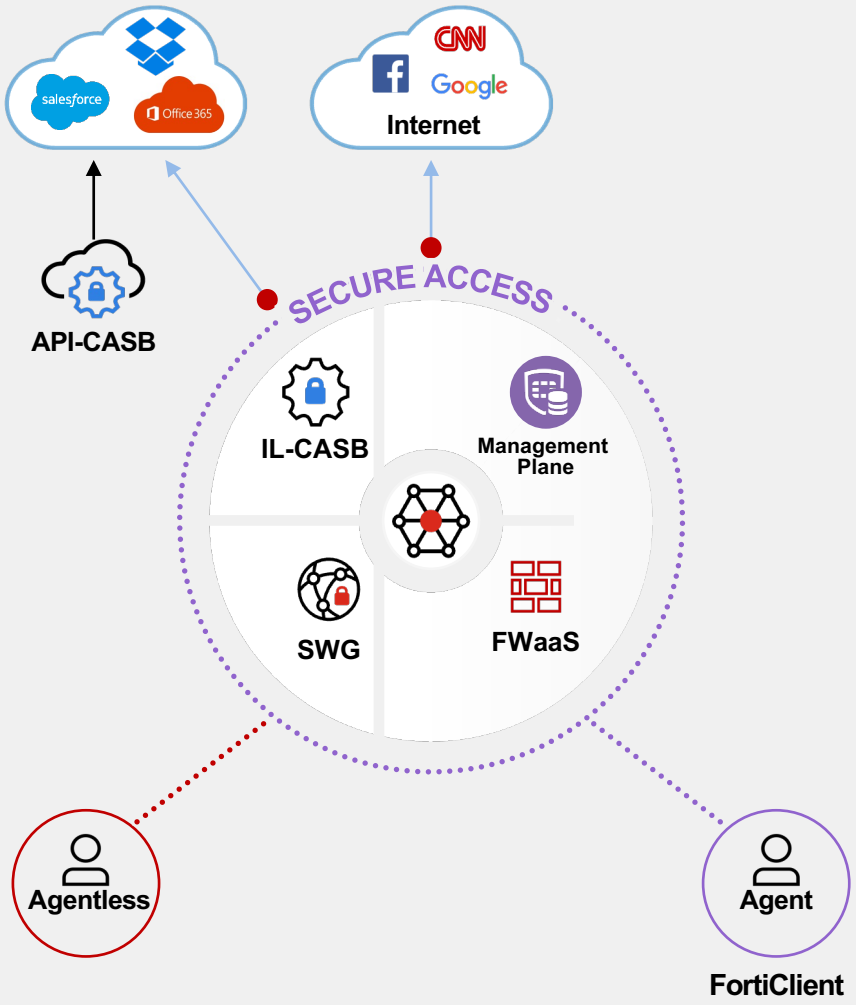
Bridge to securely connect remote users to their private applications



USE CASE 3

Secure SaaS Access for Visibility and Control

Getting to the Cloud safely



Secure Access to Cloud apps and files

Cloud App Access Control

Safe Cloud Application access and blocking of malicious apps with in-line CASB feature

Deep control & view of apps content

Control over app content and files with API-based CASB 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

Poll 2

Customer is looking to securely access voice-based applications in the data-center. Which use-case will you recommend ?

- Secure Internet Access
- Secure Private Access with ZTNA
- Secure SaaS Access
- Secure Private Access with SD-WAN Hub

Step 3 : Go To Market

What to Say and Share – Things to know about our competitors

FortiSASE: GTM- Target Customers

Engage with Existing Customers (600,000+)

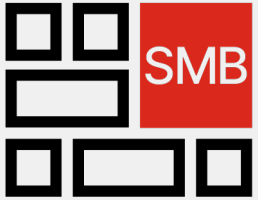
Majority of SASE deployments are brownfield, target large SD-WAN customers and ask about security posture for cloud applications and remote users.

Single Forti-OS benefits are unique to us, leverage that!

Listen for Key Drivers – SASE would be rarely asked direct!

SASE being a young technology (<3 years), a prospect coming to us and asking for SASE would be less – drivers would come from different means – SD-WAN, ZTNA, SaaS security, VPN replacement or proxy replacement

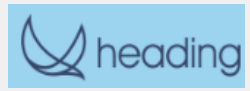
Push into SMB market



Cloud delivered aaS, Simple licensing & Operations, Strong Security Efficacy are necessary for SMB – show value with single vendor SASE offering

Trusted by Customers Globally

2023 Deal Flows

Select Customers

Vertical, location and key benefits

Education
Canada
46K users

10X
User Experience

NICE

Information Technology
Israel
10K users

50%
TCO

Healthcare
Spain
1.5K users

2 to 1
Vendor consolidation

Objection Handling

Your PoP Coverage is Limited compared with other SASE Vendors

Why is Fortinet not present in SSE MQ ?

How to Talk about SD-WAN Thin Edge Integration with FortiSASE ?

Fortinet is perceived as a hardware firewall vendor. What is special about FortiSASE ?

Competitive Landscape

Prisma Access

- Separate agents (Global Protect & Cortex XDR) required for endpoint security and traffic redirection
- Lacks secure automatic tunnel functionality for ZTNA private application access
- 3x TCO compared to FortiSASE, complex licensing model with multiple add-on services
- All security services are not available at each Prisma Access compute locations

Zscaler

- Low security efficacy; lacks 3rd party security validation
- Traffic redirection agent cannot function as EPP; need partnership with other vendors for endpoint security and SD-WAN
- App connector performance for private app access is limited to 1Gbps
- 2x TCO compared to FortiSASE, complex licensing model with multiple add-on services

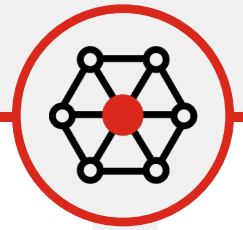
Netskope

- Cloud Firewall inspection limited for web traffic ONLY
- Netskope client-connector is a mere traffic redirection agent and doesn't offer end point protection
- Limited ZTNA posture and compliance checks for secure private application access
- Need 3rd party partnership for SD-WAN (Infiot acquisition not mature)

Cato Networks

- Relies on 3rd party security services including URL filtering, advanced threat protection
- Need partnership with other vendors for endpoint security
- Security efficacy not validated by 3rd party
- Primarily positioned from mid- and down market only

FortiSASE - The Fortinet Advantage



Secure

Users

—

Endpoints

—

Applications

Adaptive

Context-based security

—

AI-powered threat detection

Simple

Single agent

—

Configuration

—

Management

Efficient

Best-in-class

—

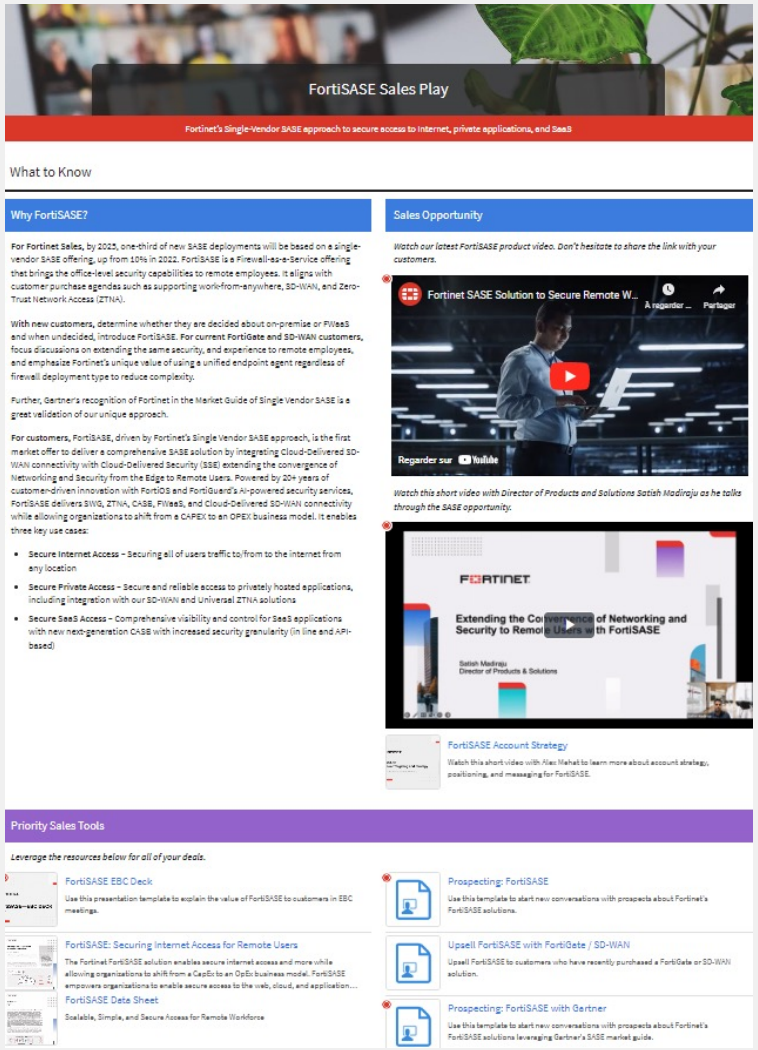
High performance

—

Integration

For more information on FortiSASE

https://fortinet.highspot.com/items/62e946367e444065271dec6f?lfrm=shp.0



- Highspot Sales Play page!
- Short SASE training on MindTickle
  - 3 videos 5-6 min each
  - https://mindtickle.app.link/rMQqTSzjnwb
- Contact us (Teams, email,…)


FORTINET

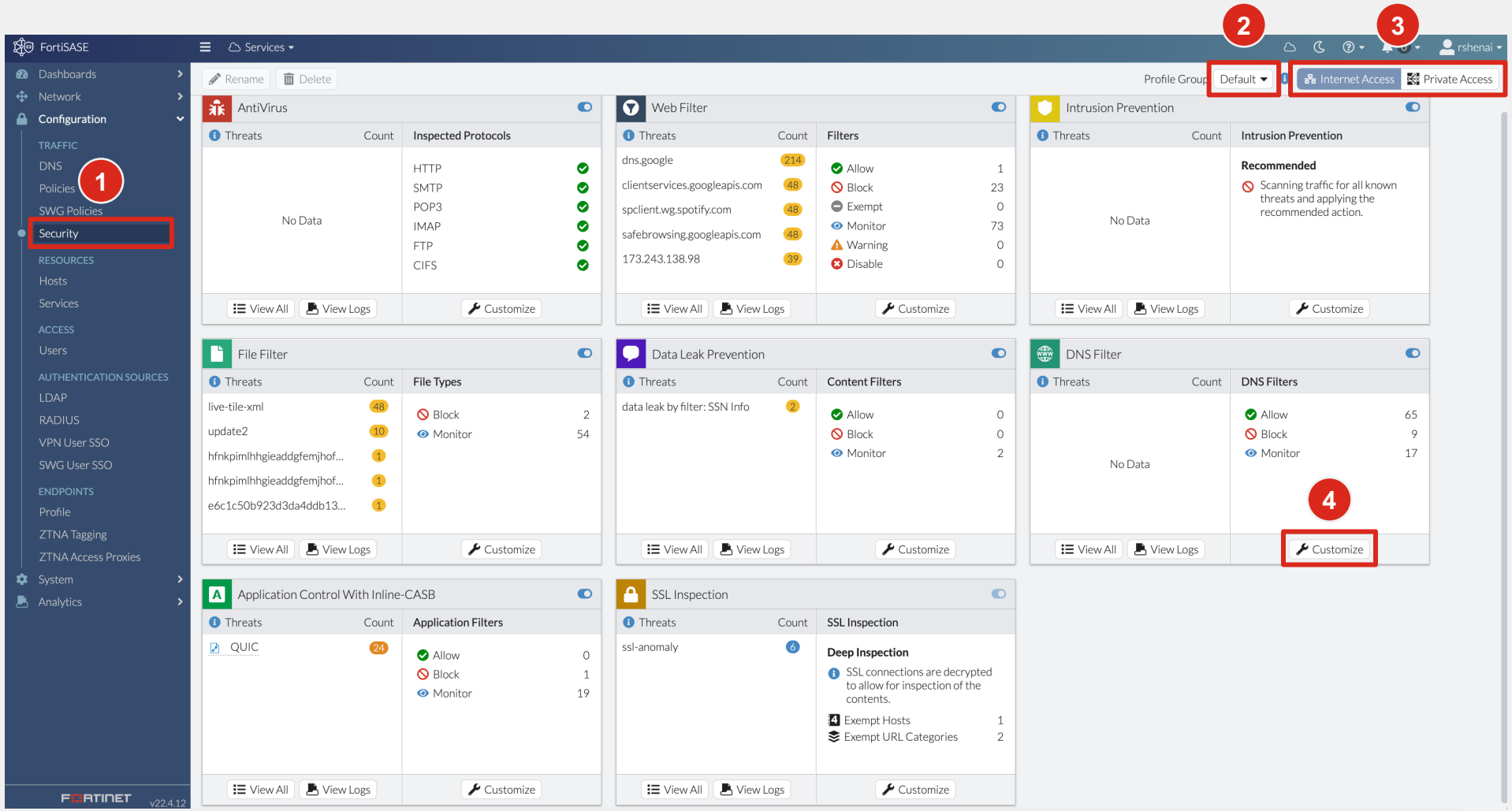
FortiExtender Thin Edge – SASE SKU

SOLUTION BUNDLE		CAT-6 LTE	CAT-7 LTE		CAT-12 LTE		CAT-16 LTE	5G SUB-6	ETHERNET WAN
			SINGLE MODEM	DUAL MODEM	SINGLE MODEM	DUAL MODEM			
	Hardware Bundle	Roadmap	Roadmap		Roadmap		Roadmap	Roadmap	Roadmap
	Renewal Bundle	Roadmap	Roadmap		Roadmap		Roadmap	Roadmap	Roadmap
FortiGate-managed	**Hardware**	FEX-101F-AM FEX-101F-EA	FEX-201F-AM FEX-201F-EA	FEX-202F-AM FEX-202F-EA	FEX-211E	FEX-212F	FEX-311F	FEX-511F	FEX-200F
	24×7 Support	FC-10-X101M-247-02-DD (FEX-101F-AM) FC-10-X101A-247-02-DD (FEX-101F-EA)	FC-10-FA21F-247-02-DD (FEX-201F-AM) FC-10-FE21F-247-02-DD (FEX-201F-EA)	FC-10-FA22F-247-02-DD (FEX-202F-AM) FC-10-FE22F-247-02-DD (FEX-202F-EA)	FC-10-F211E-247-02-DD	FC-10-X212F-247-02-DD	FC-10-X311F-247-02-DD	FC-10-X511F-247-02-DD	FC-10-X200F-247-02-DD
FortiExtender Cloud-managed	**Hardware**	FEX-101F-AM FEX-101F-EA	FEX-201F-AM FEX-201F-EA	FEX-202F-AM FEX-202F-EA	FEX-211E	FEX-212F	FEX-311F	FEX-511F	FEX-200F
	Cloud Management License*	FC-10-FEXC0-583-02-DD	FC-10-FEXC0-583-02-DD	FC-10-FEXC2-583-02-DD	FC-10-FEXC0-583-02-DD	FC-10-FEXC2-583-02-DD	FC-10-FEXC2-583-02-DD	FC-10-FEXC2-583-02-DD	FC-10-FEXC0-583-02-DD
FortiSASE Cloud-managed	**+25 Mbps**	N/A	N/A			N/A	N/A	N/A	FC1-10-FSASE-471-01-DD

What about ZTNA?

Use cases	Universal ZTNA only	FortiSASE (includes Universal ZTNA)
Secure Apps Access	Yes	Yes
SD-WAN connectivity	No	Yes
Secure Internet Access	No	Yes

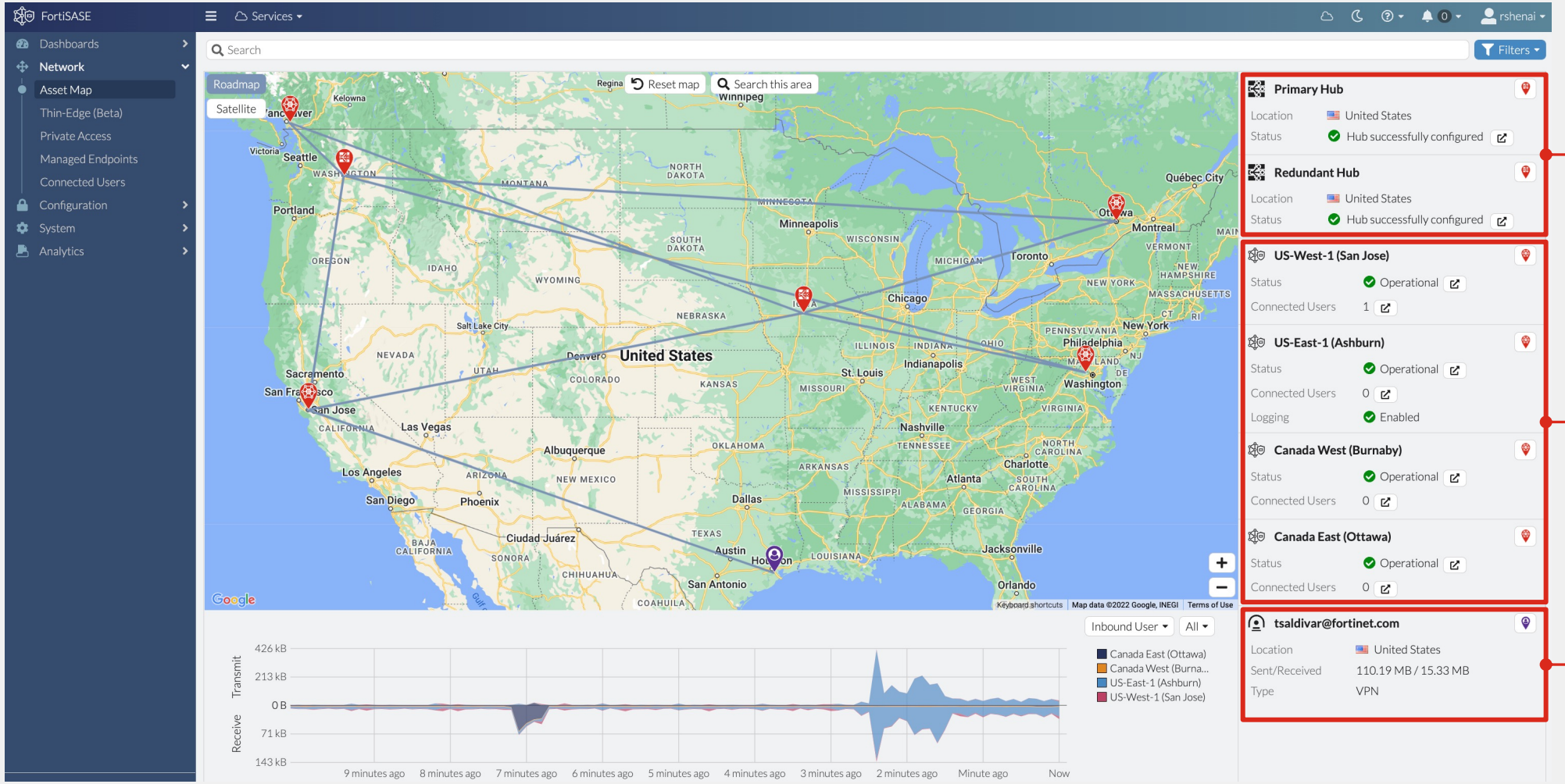
Security Configuration—One Enforcement Location



1. Simplified FOS Security from single pane
2. Default profiles available for fast consumption
3. Web and Private App visibility
4. Security profiles can be customized

FortiSASE SPA

Bridge to securely connect remote users to their private applications

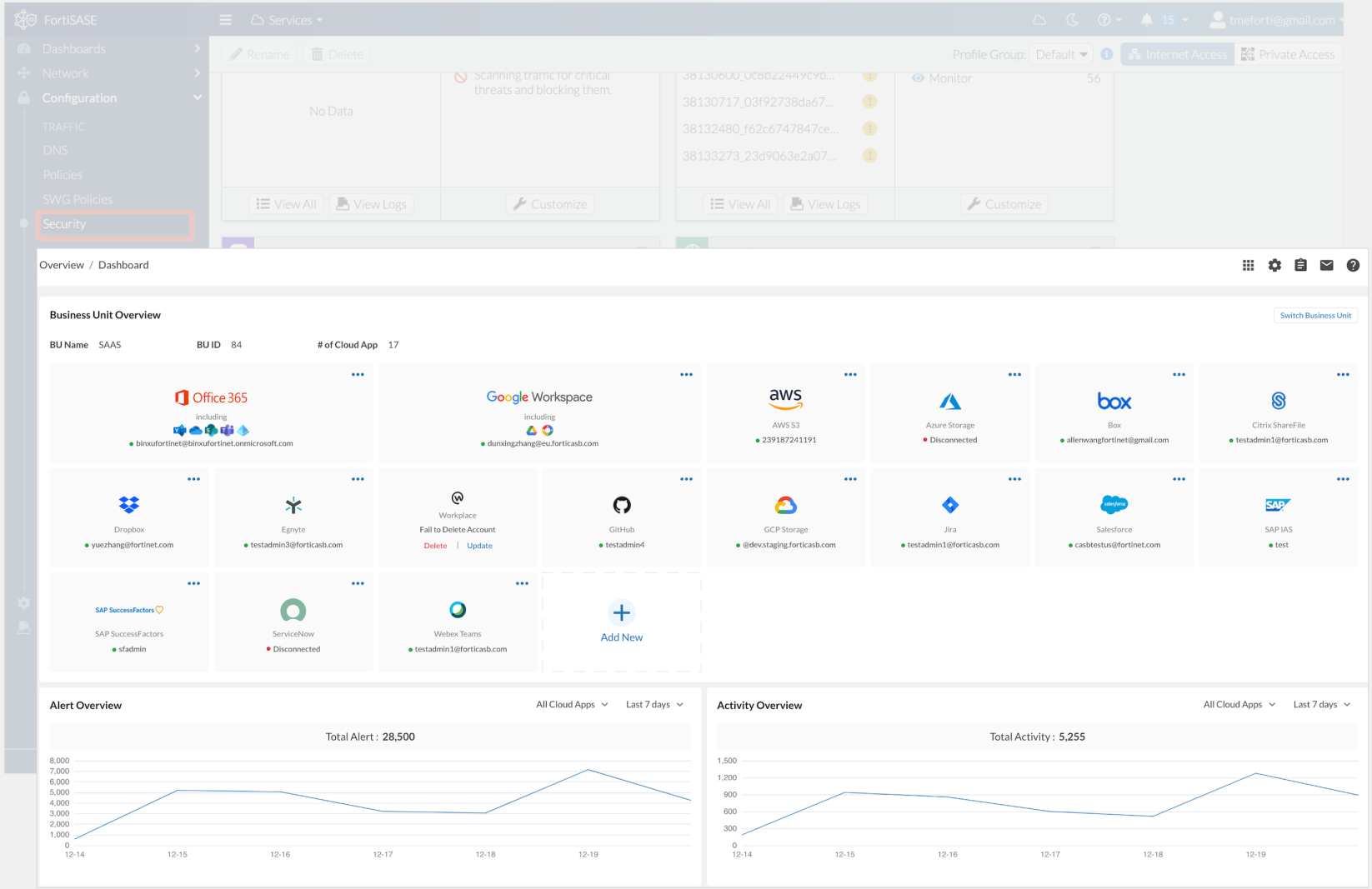


SD-WAN Datacenters

Available PoPs

Remote User

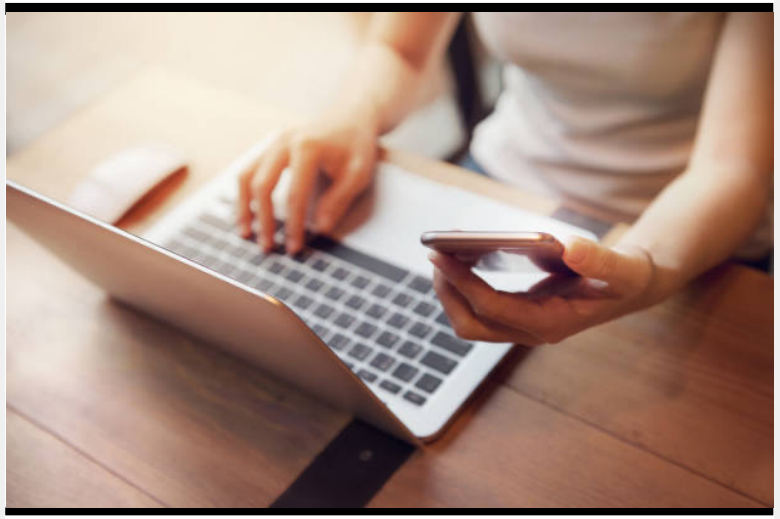
CASB: Provides Protection for Your SaaS applications



- Application status
- Activity history
- Risk statistics
- Highest risk users, files, triggered policies & countries
- Risk/usage trends

SSE components

Securely Surf the Web



Secure Web Gateway (SWG)

Firewall-as-a-Service

Safely Access Company Information

Identity-based access (ZTNA)

Securely access SaaS applications

CASB

Application control (CASB)

Objection Handling

I have never had issues with existing VPN solution

“Many employees use their office device for personal use, which can lead to infection and spread. When the VPN is then used again, these threats gain a trusted backdoor into the network. Aren't you concerned about threats moving into the network from VPN users?” VPN also provides a network wide access to that employee, if employee is compromised – entire network is at risk!

Isn’t my Fortigate enough to keep me protected?

“FortiSASE enables you to rapidly extend the same level of security to your remote employees and branches as they would have at the main office. FortiSASE offers a comprehensive set of security capabilities and efficacy backed by FortiGuard labs. It will help you: overcome security gaps with consistent security posture, deliver superior user experience with intelligent steering and dynamic routing, and simplify operations with simple cloud-delivered management and enhanced security and networking analytics”

Your PoP coverage is limited, why is that?

“Fortinet has good number of PoPs not just within US but also global – this number will keep increasing as we keep adding new customers at record pace. Each PoP is a significant investment and hence we are addressing the regions where we see SASE grow today. Additionally, all our PoPs provide security unlike our competitors. When customer/prospects ask about PoPs – steer the conversation to what pain point/ use case they are looking to solve – rarely there has been an issue due to latency with PoPs”