

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

**FORTINET**<sup>®</sup>

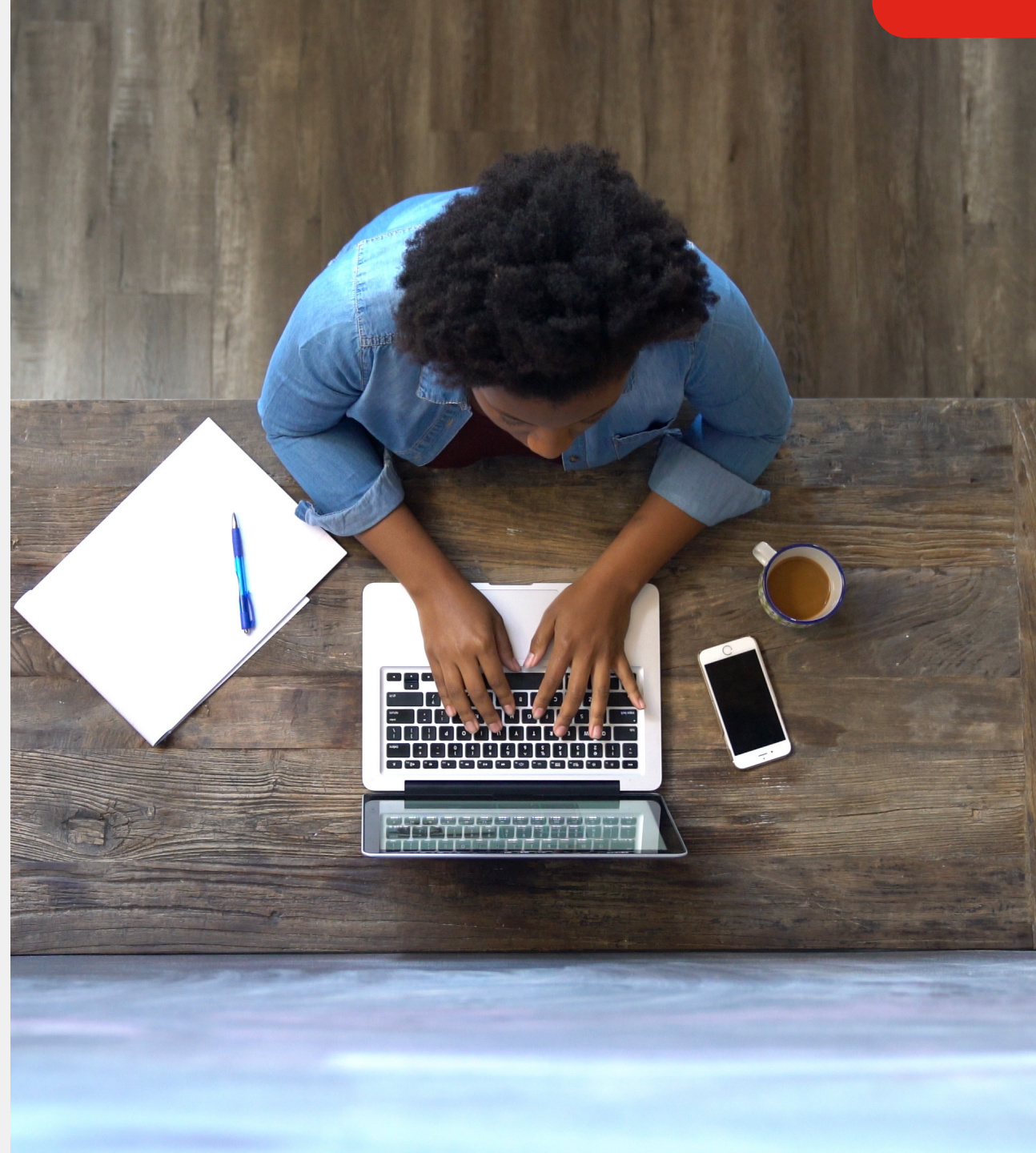
# **SASE As Easy as 1-2-3**

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



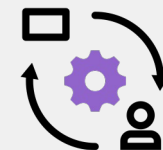
Cloud and SaaS are the new application stack



Direct Internet is the new connected network

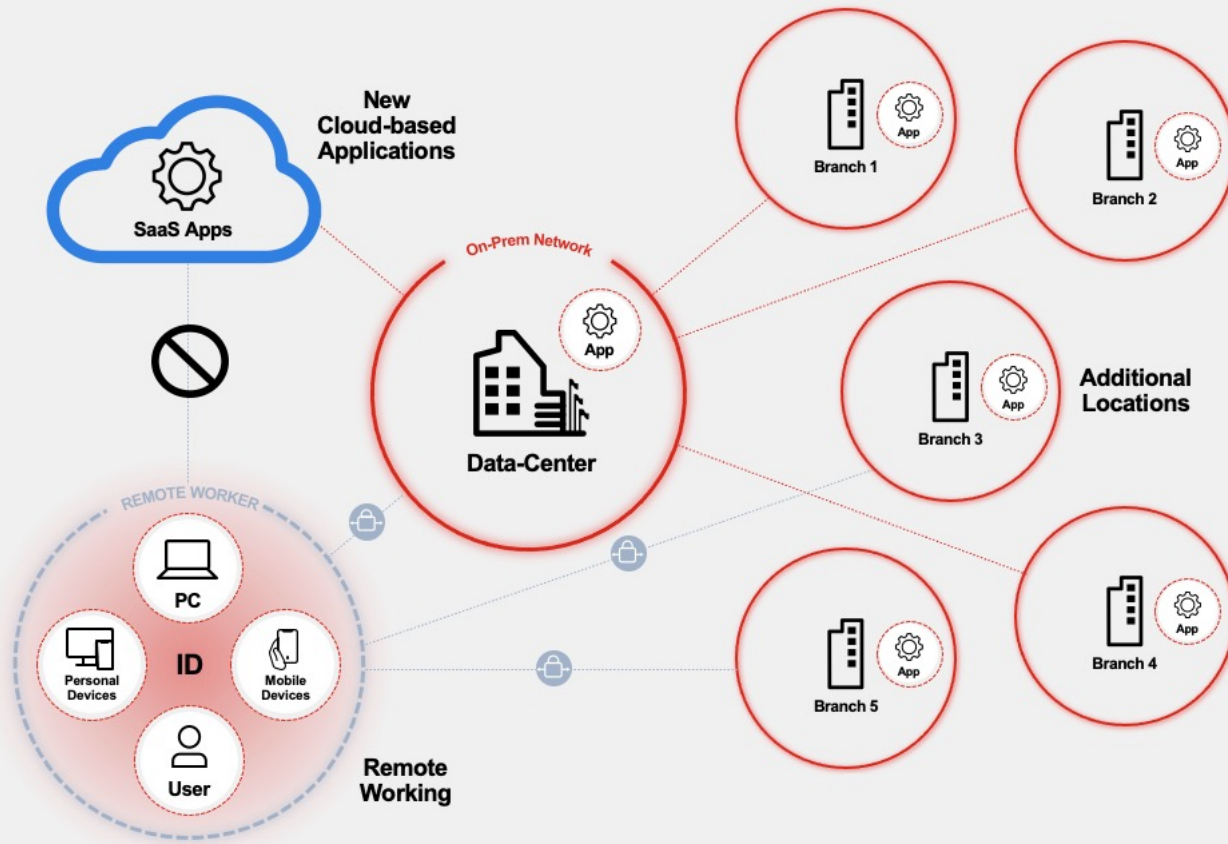


Zero Trust Mindset is the focus area for access





# 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

The Gartner logo is displayed in a large, bold, dark blue font. It consists of the word "Gartner" followed by a registered trademark symbol (®).

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

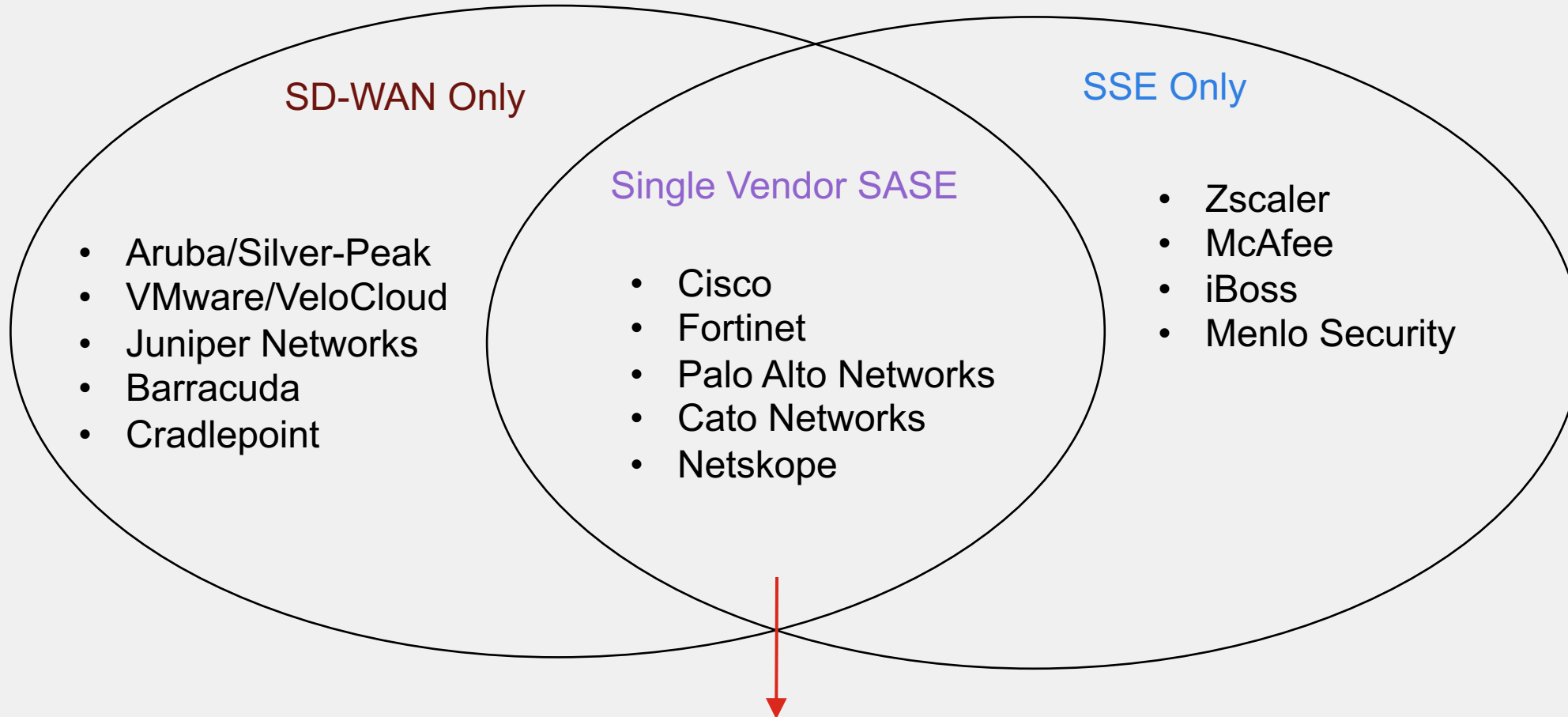
Monitors outbound network traffic for unauthorized sensitive data exfiltration (eg. credit card nb)

Single Vendor SASE	
SD-WAN	SSE
<ul style="list-style-type: none"><li>• On-prem device</li><li>• WAN Edge</li><li>• Routing</li><li>• Quality of Service</li></ul>	<ul style="list-style-type: none"><li>• Cloud-delivered</li><li>• SWG</li><li>• FWaaS</li><li>• ZTNA</li><li>• CASB</li><li>• DLP</li></ul>





# 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



## 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](#)

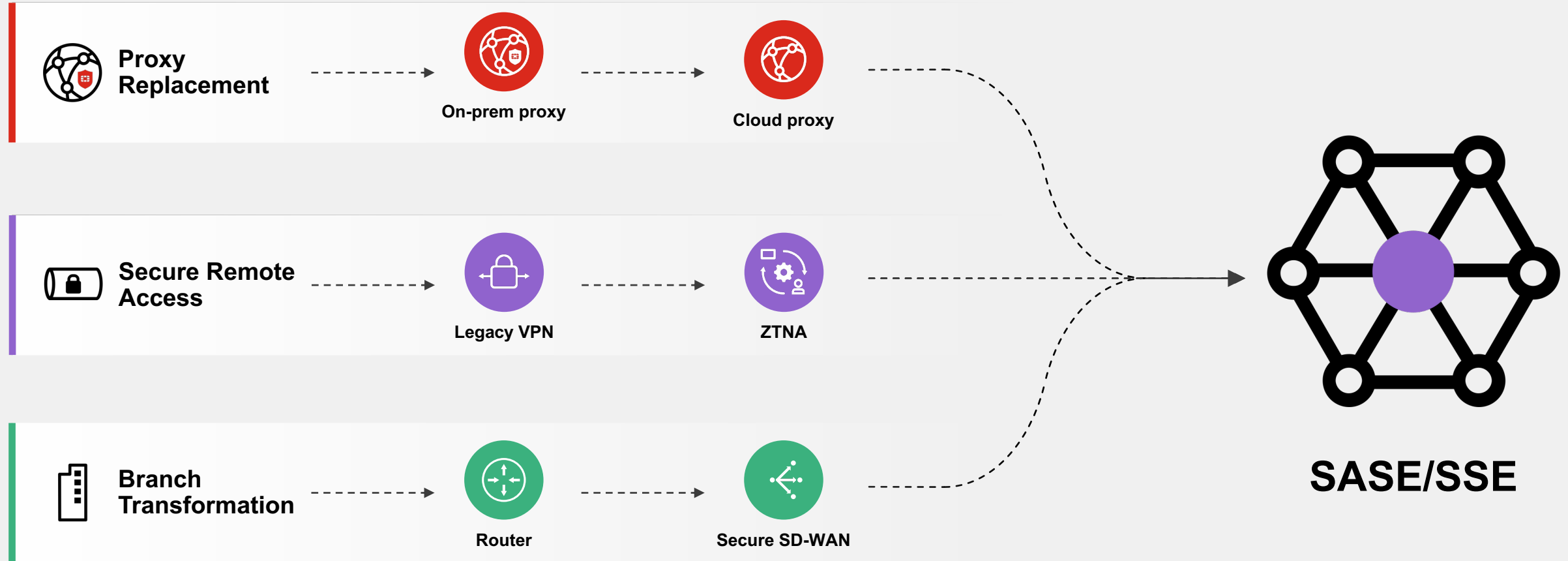
Single-vendor SASE delivers converged network and security capabilities to connect and secure distributed users, devices and locations to resources in the cloud, edge and on-premises. Infrastructure and operations leaders should use this research to analyze the emerging single-vendor SASE market.



## 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



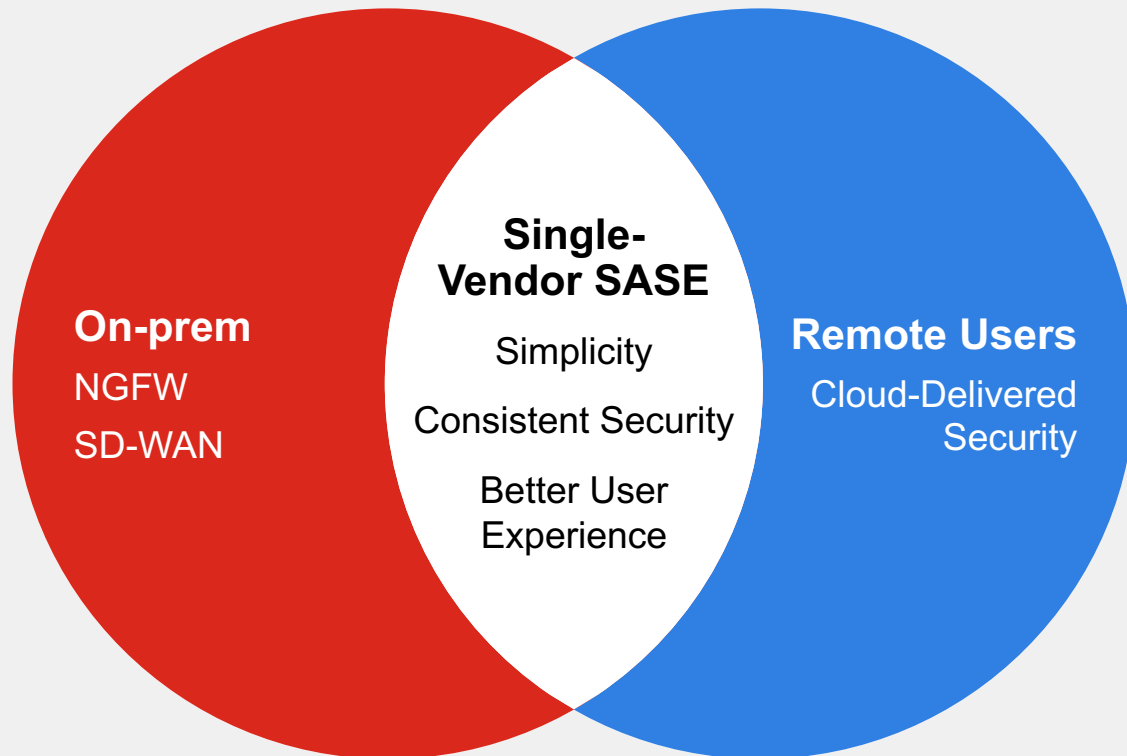


# Step 2 : Introduce Fortinet SASE

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**



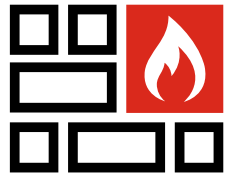
**Unified FortiClient Agent**

# Pragmatic Journey to SASE

With Fortinet's convergence of security and networking everywhere

1

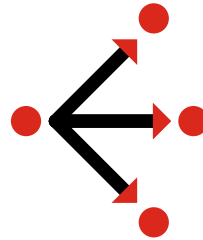
Secure Edge  
Connectivity



NGFW

2

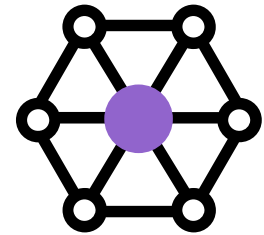
Optimize Application  
Experience



SD-WAN

3

Secure  
Remote Users



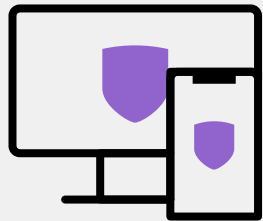
SASE



# FortiSASE – Cloud Delivered Convergence

Cloud-delivered security with Integration with On-Prem Networking

## Securing Remote Users



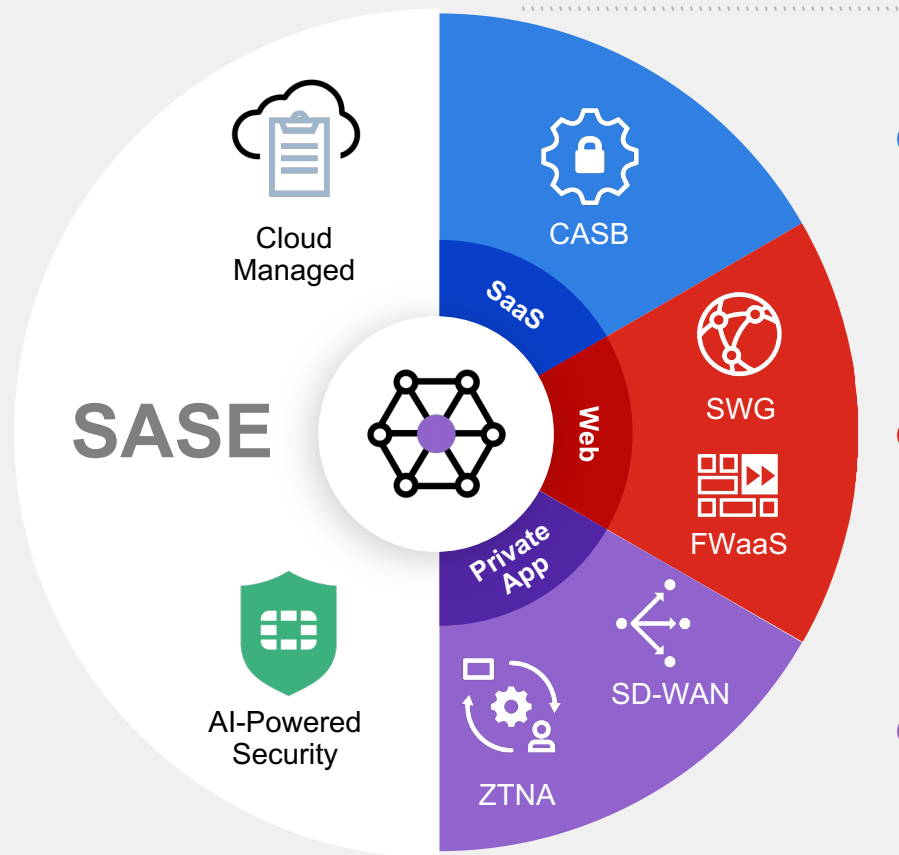
FortiClient Unified Agent

## Securing Thin Edges



FortiExtender

## Cloud-delivered Security & Networking



## Improved User Experience

Secure SaaS Access



Secure Internet Access

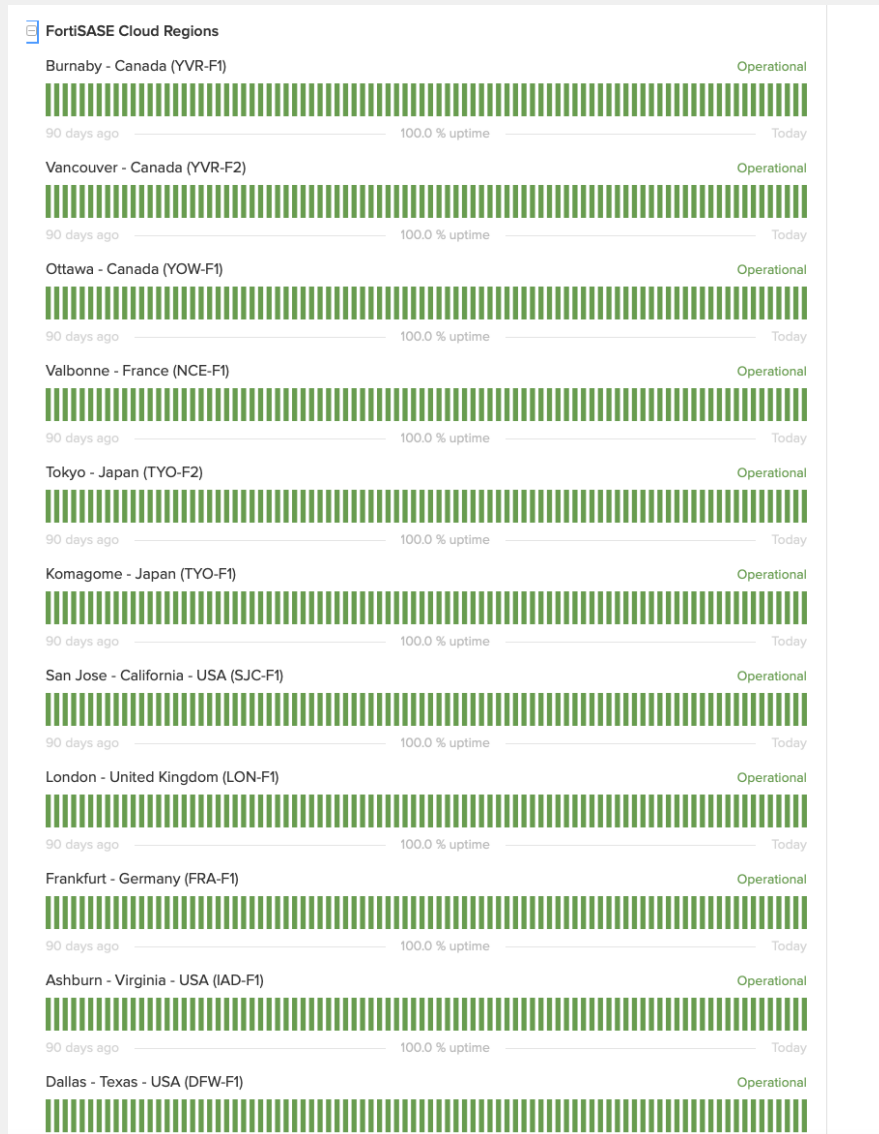


Secure Private Access





# 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

[Link to Ordering Guide](#)

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

### 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

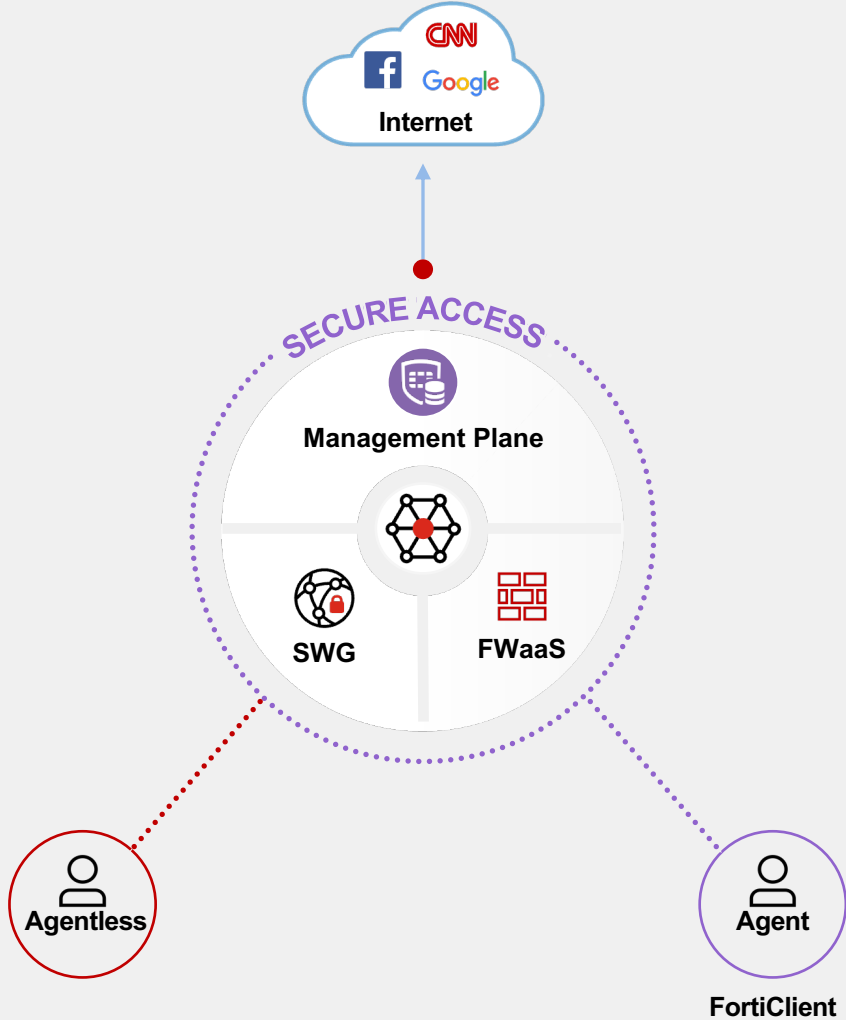
2 – Analytics and Visibility

3 – On-boarding users



# 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

The screenshot displays the FortiSASE Security Configuration interface. The left sidebar shows the 'Security' menu highlighted with a red box and a red circle labeled '1'. The main content area is divided into several security modules, each with a 'Threats' table and a 'Filters' table. A 'Profile Group' dropdown menu is highlighted with a red box and a red circle labeled '2', showing options for 'Default', 'Internet Access', and 'Private Access' (the latter two are also highlighted with a red box and a red circle labeled '3'). A 'Customize' button in the bottom right of the DNS Filter module is highlighted with a red box and a red circle labeled '4'.

Threats	Count	Inspected Protocols
No Data		HTTP, SMTP, POP3, IMAP, FTP, CIFS

Threats	Count	Filters
dns.google	214	Allow (1), Block (23), Exempt (0), Monitor (73), Warning (0), Disable (0)
clientservices.googleapis.com	48	
spclient.wg.spotify.com	48	
safebrowsing.googleapis.com	48	
173.243.138.98	39	

Threats	Count	Intrusion Prevention
No Data		Recommended: Scanning traffic for all known threats and applying the recommended action.

Threats	Count	File Types
live-tile-xml	48	Block (2), Monitor (54)
update2	10	
hfnpimlhhgieaddgfemjhof...	1	
hfnpimlhhgieaddgfemjhof...	1	
e6c1c50b923d3da4ddb13...	1	

Threats	Count	Content Filters
data leak by filter: SSN Info	2	Allow (0), Block (0), Monitor (2)

Threats	Count	DNS Filters
No Data		Allow (65), Block (9), Monitor (17)

Threats	Count	Application Filters
QUIC	24	Allow (0), Block (1), Monitor (19)

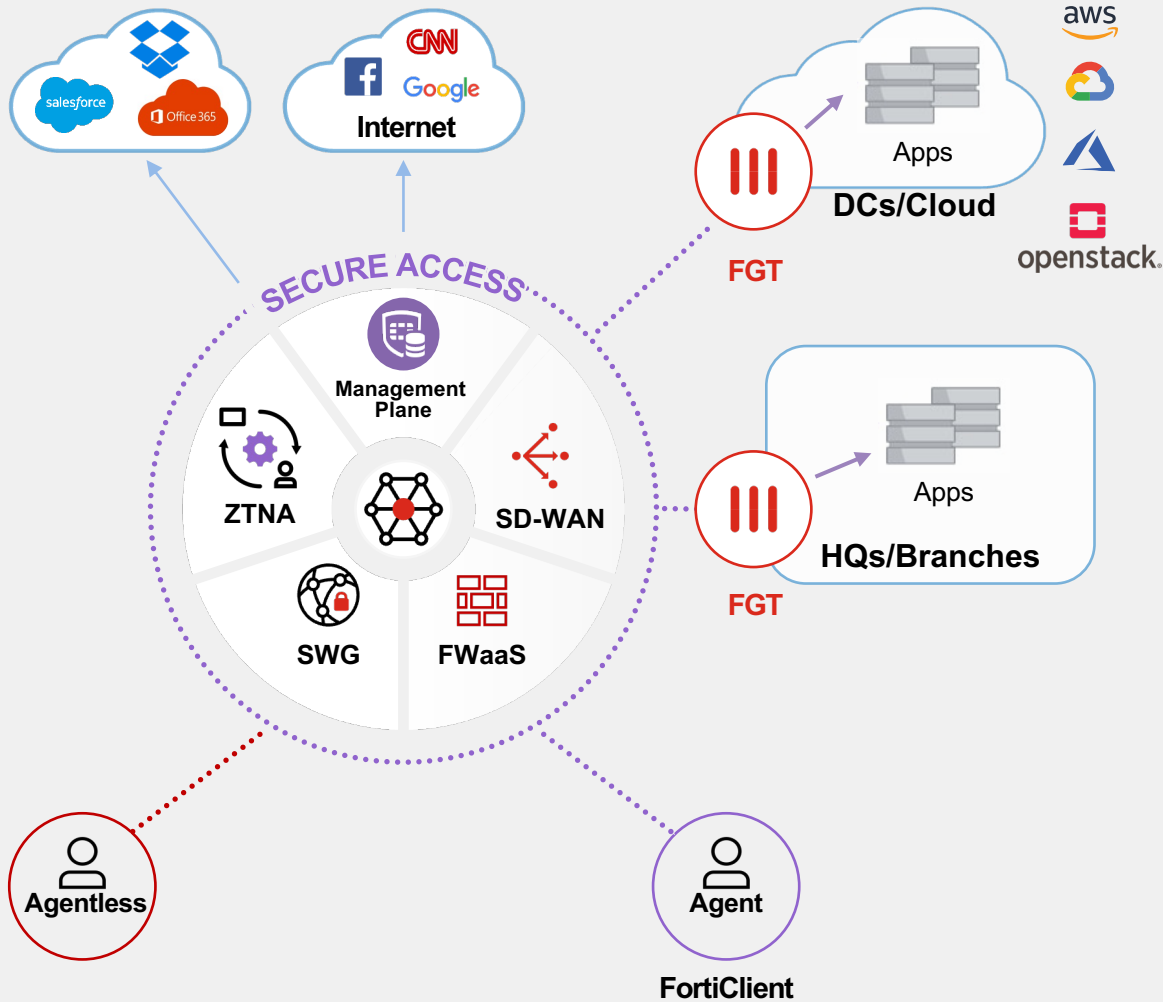
Threats	Count	SSL Inspection
ssl-anomaly	6	Deep Inspection: SSL connections are decrypted to allow for inspection of the contents. Exempt Hosts (1), Exempt URL Categories (2)

- 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



# Flexible Secure Access to corporate applications

Getting to the corporate applications safely



## Secure corporate app access



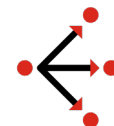
### Secure Cloud & datacenter app access

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

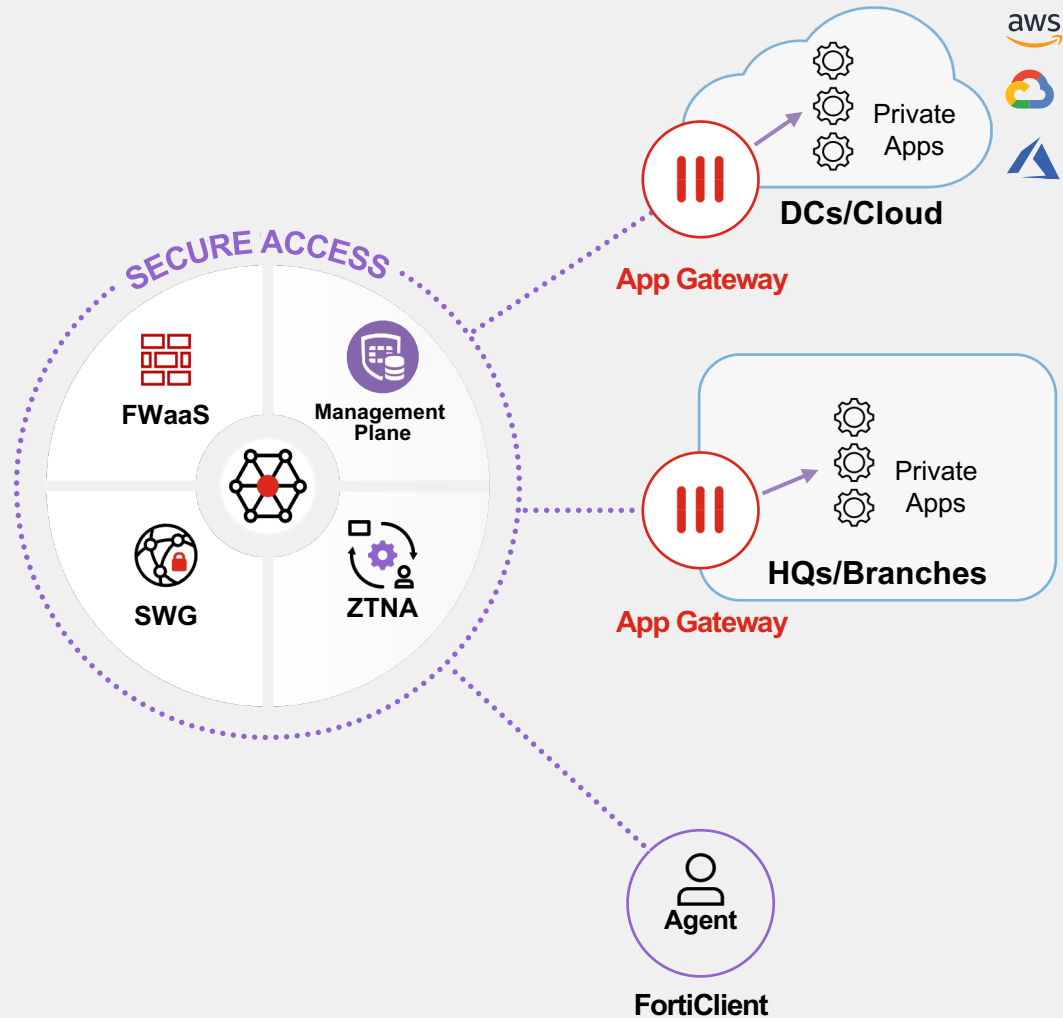


### On-prem SD-WAN integration

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

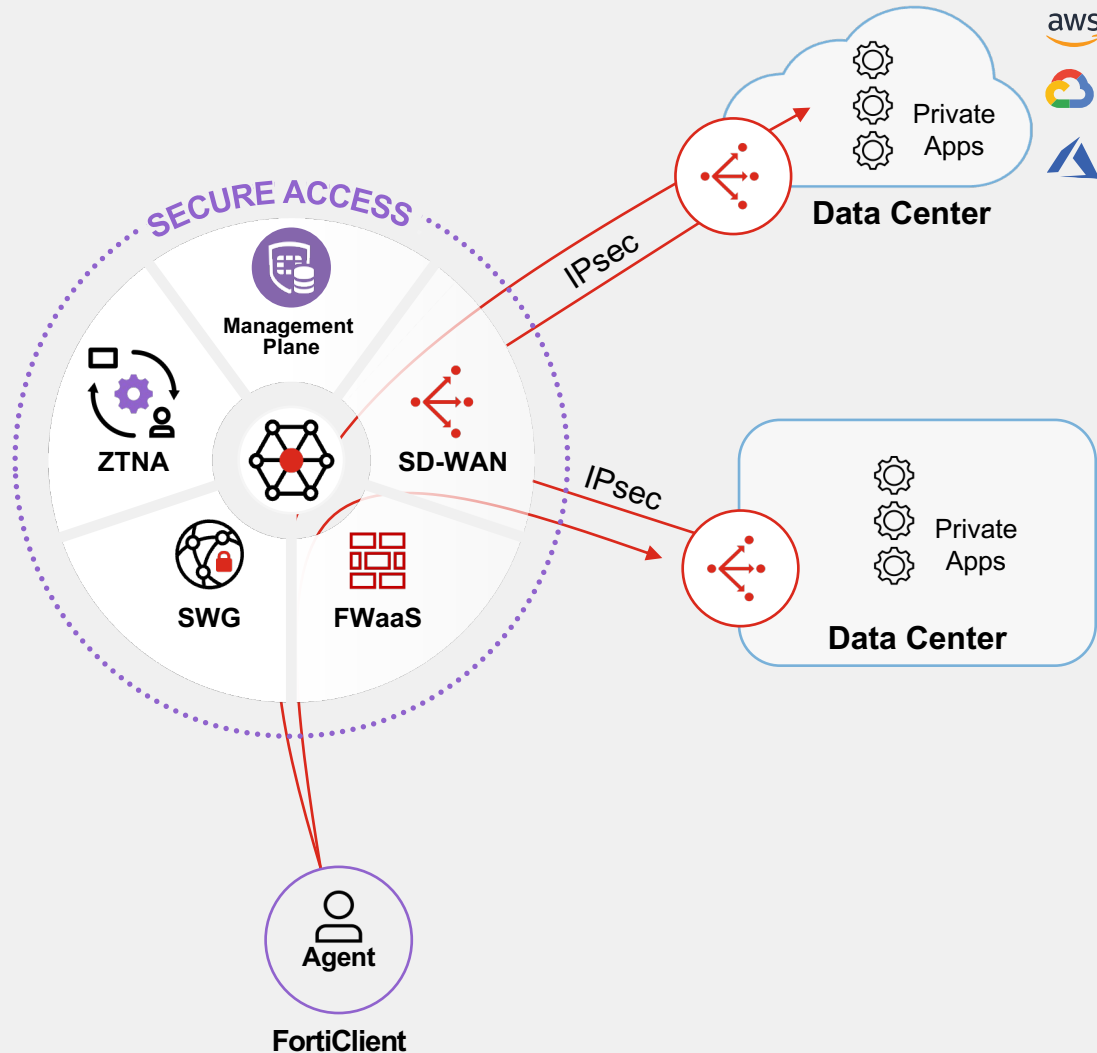


Granular per-session  
posture checks



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

The screenshot displays the FortiSASE interface with a map of the United States. The map shows several SD-WAN hubs and available PoPs. A remote user, 'tsaldivar@fortinet.com', is shown connected to the US-East-1 (Ashburn) PoP. The interface includes a sidebar with navigation options, a search bar, and a status panel on the right.

**SD-WAN Datacenters:**

- Primary Hub:** Location: United States, Status: Hub successfully configured
- Redundant Hub:** Location: United States, Status: Hub successfully configured

**Available PoPs:**

- US-West-1 (San Jose):** Status: Operational, Connected Users: 1
- US-East-1 (Ashburn):** Status: Operational, Connected Users: 0, Logging: Enabled
- Canada West (Burnaby):** Status: Operational, Connected Users: 0
- Canada East (Ottawa):** Status: Operational, Connected Users: 0

**Remote User:**

- tsaldivar@fortinet.com:** Location: United States, Sent/Received: 110.19 MB / 15.33 MB, Type: VPN

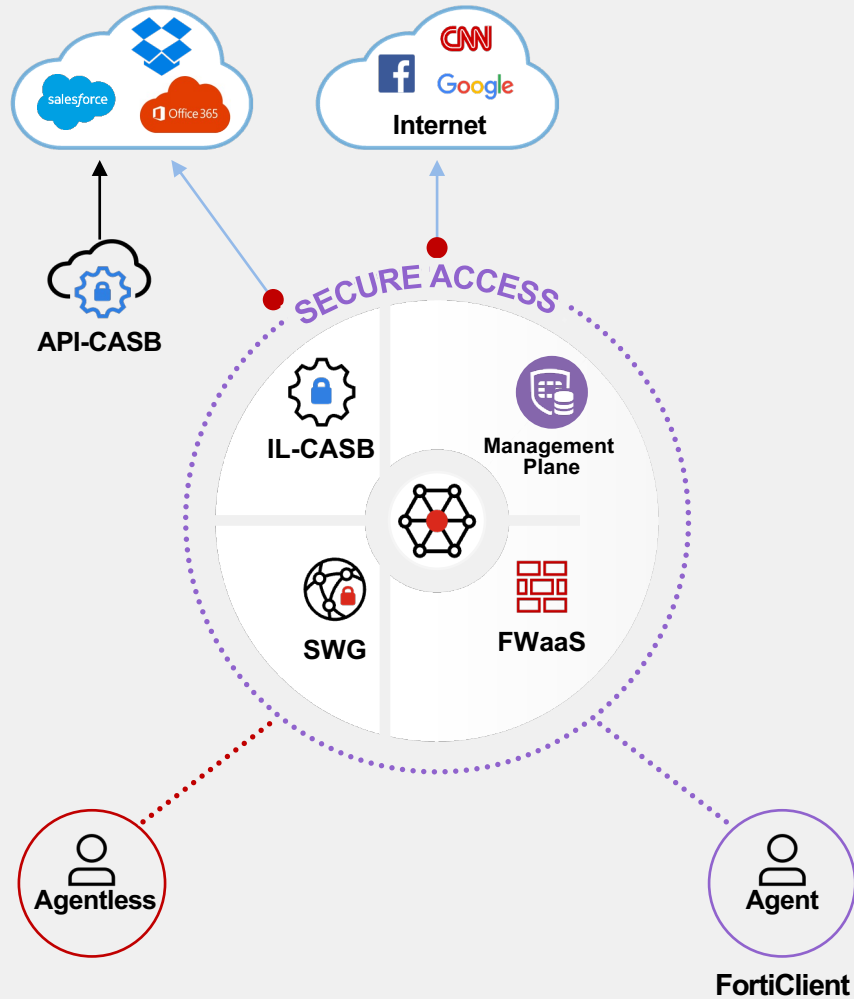
**Network Performance Graph:**

The graph shows network performance metrics over time. The Y-axis represents Receive and Transmit data in kB, ranging from 0B to 426 kB. The X-axis shows time intervals from 9 minutes ago to Now. The legend indicates data for Canada East (Ottawa), Canada West (Burnaby), US-East-1 (Ashburn), and US-West-1 (San Jose).



# 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





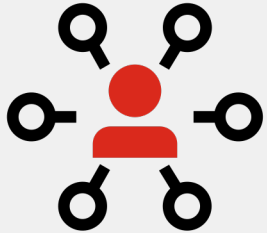
# Step 3 : Go To Market

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



# FortiSASE: GTM- Target Customers

## Engage with Existing Customers (600,000+)



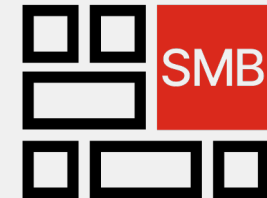
Majority of SASE deployments are brownfield, target large SD-WAN customers and ask about security posture for cloud applications and remote users. Single Forti-OS benefits are unique to us, leverage that!

## 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



Confidential- Under NDA only

© Fortinet Inc. All Rights Reserved.

# Select Customers

Vertical, location and key benefits



Upper Grand  
District School Board

---

## 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 3<sup>rd</sup> 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 3<sup>rd</sup> party partnership for SD-WAN (Infiot acquisition not mature )

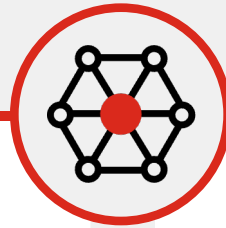


## Cato Networks

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

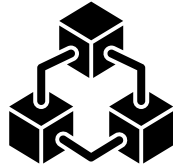


# FortiSASE - The Fortinet Advantage



**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>

**FortiSASE Sales Play**  
Fortinet's Single-Vendor SASE approach to secure access to internet, private applications, and SaaS

**What to Know**

**Why FortiSASE?**

For Fortinet Sales, by 2023, one-third of new SASE deployments will be based on a single-vendor SASE offering, up from 10% in 2022. FortiSASE is a Firewall-as-a-Service offering that brings the office-level security capabilities to remote employees. It aligns with customer purchase agendas such as supporting work-from-anywhere, SD-WAN, and Zero-Trust Network Access (ZTNA).

With new customers, determine whether they are decided about on-premise or PaaS and when undecided, introduce FortiSASE. For current FortiGate and SD-WAN customers, focus discussions on extending the same security, and experience to remote employees, and emphasize Fortinet's unique value of using a unified endpoint agent regardless of firewall deployment type to reduce complexity.

Further, Gartner's recognition of Fortinet in the Market Guide of Single Vendor SASE is a great validation of our unique approach.

For customers, FortiSASE, driven by Fortinet's Single Vendor SASE approach, is the first market offer to deliver a comprehensive SASE solution by integrating Cloud-Delivered SD-WAN connectivity with Cloud-Delivered Security (CDS) extending the convergence of Networking and Security from the Edge to Remote Users. Powered by 20+ years of customer-driven innovation with FortiOS and FortiGuard's AI-powered security services, FortiSASE delivers SaaS, ZTNA, CDS, Private, and Cloud-Delivered SD-WAN connectivity while allowing organizations to shift from a CapEx to an OpEx business model. It enables three key use cases:

- Secure Internet Access – Securing all of users traffic to/from the Internet from any location
- Secure Private Access – Secure and reliable access to privately hosted applications, including integration with our SD-WAN and Universal ZTNA solutions
- Secure SaaS Access – Comprehensive visibility and control for SaaS applications with next-generation CASB with increased security granularity (in line and API-based)

**Sales Opportunity**

Watch our latest FortiSASE product video. Don't hesitate to share the link with your customers.

**Fortinet SASE Solution to Secure Remote W...**

Watch this short video with Director of Products and Solutions Satish Madiraju as he talks through the SASE opportunity.

**FortiSASE Account Strategy**

Watch this short video with Alex Hallett to learn more about account strategy, positioning, and messaging for FortiSASE.

**Priority Sales Tools**

Leverage the resources below for all of your deals.

- FortiSASE EBC Deck**  
Use this presentation template to explain the value of FortiSASE to customers in EBC meetings.
- Prospecting: FortiSASE**  
Use this template to start new conversations with prospects about Fortinet's FortiSASE solutions.
- FortiSASE: Securing Internet Access for Remote Users**  
The Fortinet FortiSASE solution enables secure internet access and more while allowing organizations to shift from a CapEx to an OpEx business model. FortiSASE empowers organizations to enable secure access to the web, cloud, and application...
- Upsell FortiSASE with FortiGate / SD-WAN**  
Upsell FortiSASE to customers who have recently purchased a FortiGate or SD-WAN solution.
- FortiSASE Data Sheet**  
Scalable, Simple, and Secure Access for Remote Workforce
- Prospecting: FortiSASE with Gartner**  
Use this template to start new conversations with prospects about Fortinet's FortiSASE solutions leveraging Gartner's SASE market guide.

- Highspot Sales Play page!
- Short SASE training on MindTickle
  - 3 videos 5-6 min each
  - <https://mindtickle.app.link/rMQqTSzjnw>
- 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			
<b>Hardware Bundle</b>	Roadmap		Roadmap		Roadmap		Roadmap	Roadmap	Roadmap
<b>Renewal Bundle</b>	Roadmap		Roadmap		Roadmap		Roadmap	Roadmap	Roadmap
<b>FortiGate-managed</b>	<b>Hardware</b>	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
	<b>24x7 Support</b>	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
<b>FortiExtender Cloud-managed</b>	<b>Hardware</b>	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
	<b>Cloud Management License*</b>	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
<b>FortiSASE Cloud-managed</b>	<b>+25 Mbps</b>	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

The screenshot displays the FortiSASE Security Configuration interface. The left sidebar shows the 'Security' menu item highlighted with a red box and a red circle containing the number '1'. At the top right, the 'Profile Group' dropdown is set to 'Default', with 'Internet Access' and 'Private Access' options also visible, highlighted with a red box and a red circle containing the number '2'. The main area contains several security modules, each with a 'Customize' button highlighted by a red box and a red circle containing the number '4'. The modules shown are:

- AntiVirus**: Shows 'Threats' as 'No Data' and 'Inspected Protocols' including HTTP, SMTP, POP3, IMAP, FTP, and CIFS, all with green checkmarks.
- Web Filter**: Shows 'Threats' with a list of domains and their counts (e.g., dns.google: 214) and 'Filters' including Allow, Block, Exempt, Monitor, Warning, and Disable.
- Intrusion Prevention**: Shows 'Threats' as 'No Data' and 'Intrusion Prevention' with a 'Recommended' action: 'Scanning traffic for all known threats and applying the recommended action.'
- File Filter**: Shows 'Threats' with file types and counts (e.g., live-tile-xml: 48) and 'File Types' including Block and Monitor.
- Data Leak Prevention**: Shows 'Threats' with a count of 2 for 'data leak by filter: SSN Info' and 'Content Filters' including Allow, Block, and Monitor.
- DNS Filter**: Shows 'Threats' as 'No Data' and 'DNS Filters' including Allow, Block, and Monitor.
- Application Control With Inline-CASB**: Shows 'Threats' with a count of 24 for 'QUIC' and 'Application Filters' including Allow, Block, and Monitor.
- SSL Inspection**: Shows 'Threats' with a count of 6 for 'ssl-anomaly' and 'SSL Inspection' including 'Deep Inspection' (SSL connections are decrypted) and 'Exempt Hosts' and 'Exempt URL Categories'.

- 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

The screenshot displays the FortiSASE SPA interface. On the left is a navigation menu with options: Dashboards, Network, Asset Map, Thin-Edge (Beta), Private Access, Managed Endpoints, Connected Users, Configuration, System, and Analytics. The main area features a map of the United States with several locations marked as SD-WAN Datacenters and Available PoPs. A legend at the bottom right of the map identifies the locations: Canada East (Ottawa) in blue, Canada West (Burnaby) in orange, US-East-1 (Ashburn) in green, and US-West-1 (San Jose) in red. A red box highlights the Primary Hub, Redundant Hub, and the four Available PoPs. A red line connects these hubs and PoPs to the label 'SD-WAN Datacenters' and 'Available PoPs'. Another red box highlights the Remote User profile for 'tsaldivar@fortinet.com', which is connected to the US-East-1 (Ashburn) PoP. A red line connects this profile to the label 'Remote User'. At the bottom of the interface is a network traffic graph showing Receive and Transmit data over time, with a legend for the same four locations as the map.

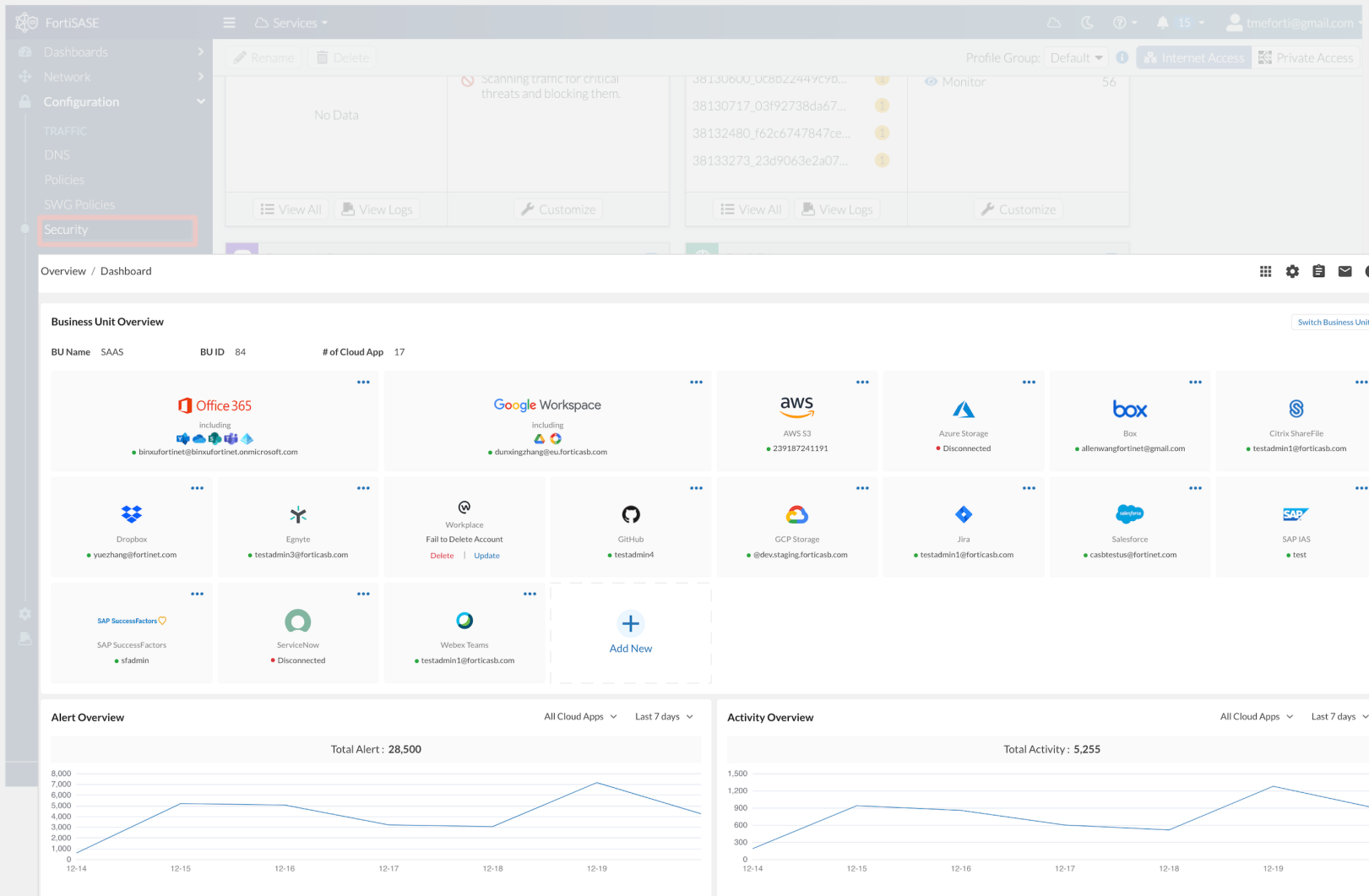
Location	Status	Connected Users	Logging
Primary Hub	Hub successfully configured		
Redundant Hub	Hub successfully configured		
US-West-1 (San Jose)	Operational	1	
US-East-1 (Ashburn)	Operational	0	Enabled
Canada West (Burnaby)	Operational	0	
Canada East (Ottawa)	Operational	0	

Location	Status	Sent/Received	Type
tsaldivar@fortinet.com	Operational	110.19 MB / 15.33 MB	VPN





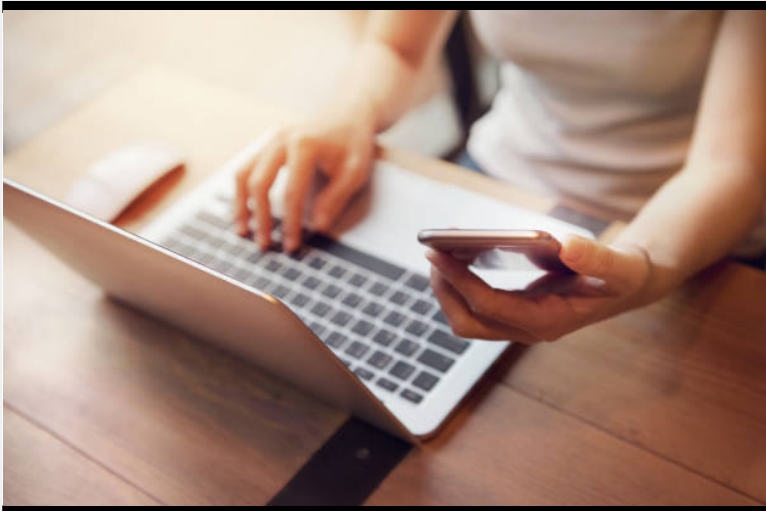
# CASB: Provides Protection for Your SaaS applications



- 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



**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”

