



# SASE Basics

What is SASE

Use Cases

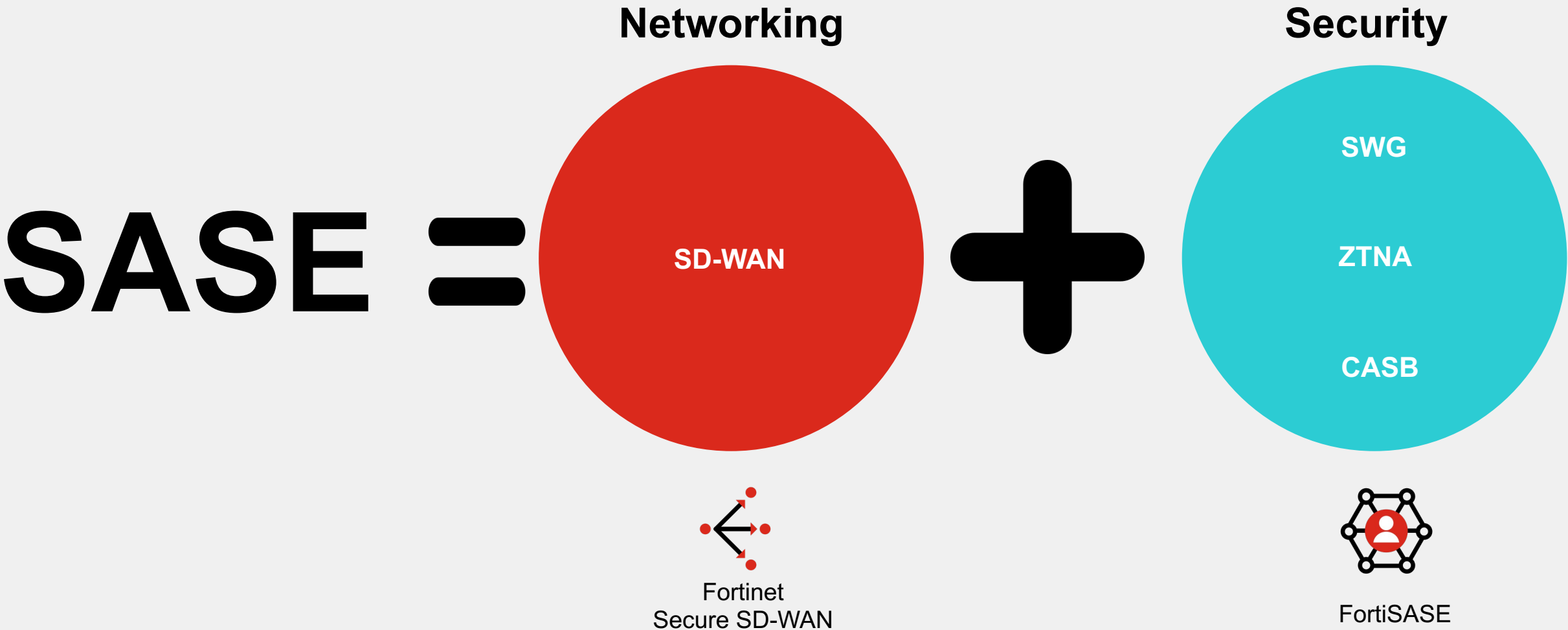
UI

Licensing

FAQs



# Gartner SASE Definition : Simplified



# FortiSASE – FortiGate as a Service

## FortiGate



FortiGate Hardware Appliance  
Accelerated by Security  
Processing Unit (SPU)



System  
on a Chip



Network  
Processor



Content  
Processor

## FortiGate VM



FortiGate Virtual Machine  
Licensed by CPU Cores



1-92  
Cores



1-72  
Cores



1-32  
Cores



1-32  
Cores

## FortiSASE



FortiGate Delivered as a  
Cloud Service



Remote  
Users



Branch  
Office



# Comprehensive Cloud-Delivered Security



**Web Filtering**

**Intrusion Prevention System**



**DNS Filtering**

**Sandboxing**



**SSL Inspection**

**Anti-Virus**

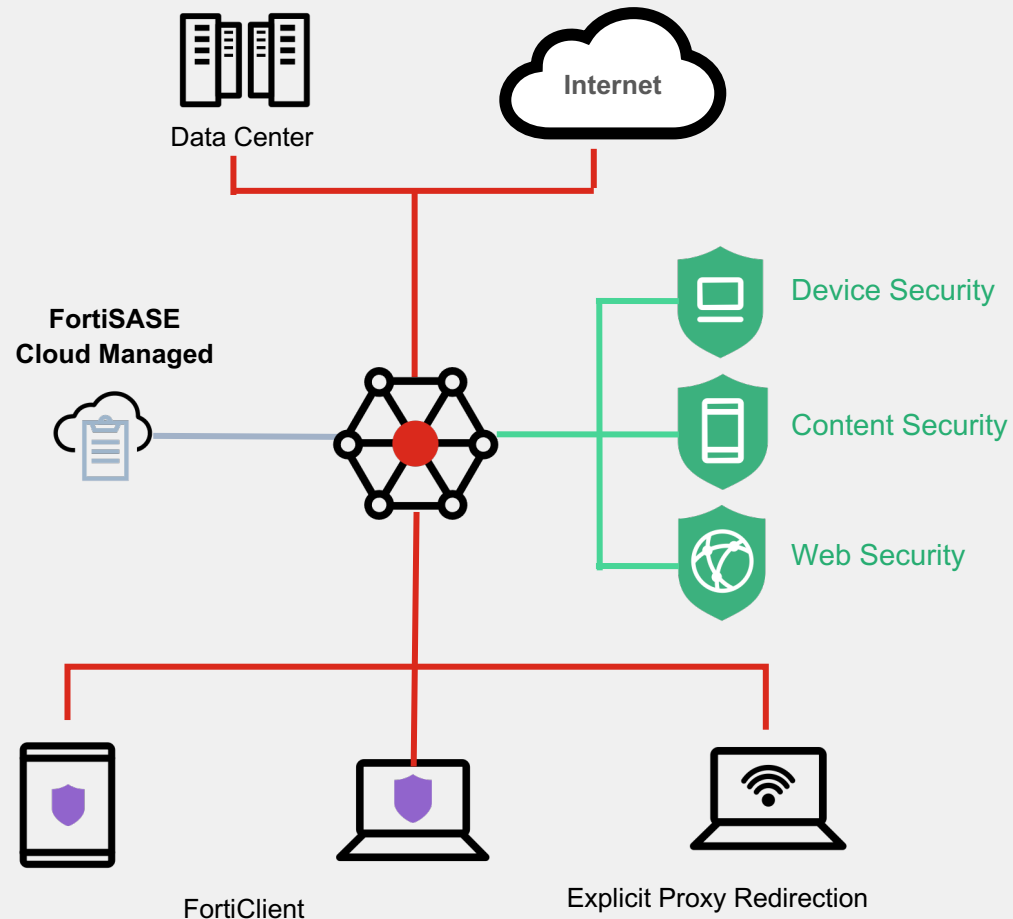


# Fast Expanding Global PoP Coverage....More In Pipeline

Region	Locations
North America	Burnaby, Canada Ottawa, Canada Vancouver, Canada Ashburn, US San Jose, US Dallas, US
EMEA	Sophia, France Paris, France Frankfurt, Germany London, UK
APAC	Tokyo, Japan Tokyo, Japan (2 <sup>nd</sup> ) Singapore, Singapore



# FortiSASE: Key Use Cases

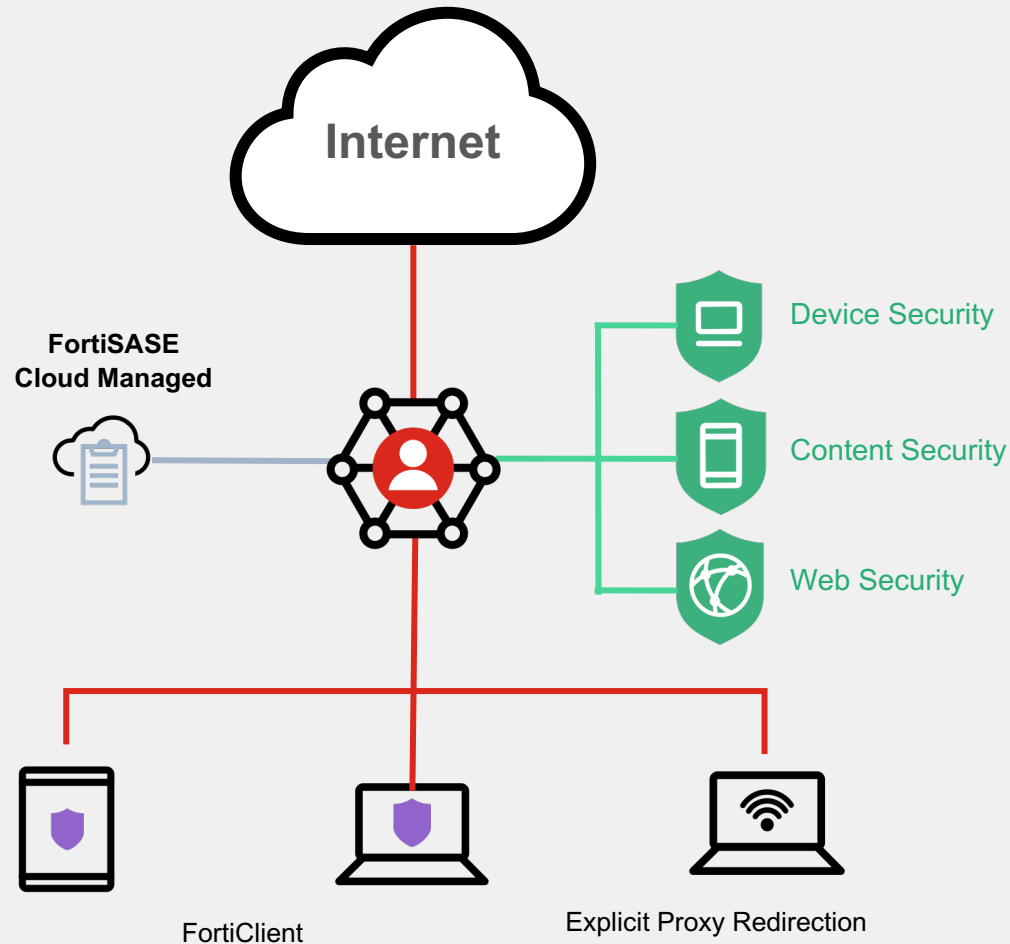


**Secure Internet Access (Agent & Agentless)**

**Secure Private Access to Corporate Apps**

**Cloud-based Management & Simple Licensing**

# Use Case 1: Secure Internet Access (Agent & Agentless)



## WHY it matters

53% of the workforce will work hybrid post COVID

## HOW we solve it

- Traffic redirection based on Agent(FortiClient) or Explicit Proxy(PAC file)
- Identity-based policies per user/user Groups
- Deep AD integration for user mapping

## BENEFITS

- Secure Remote Users everywhere
- Integrated for Superior Endpoint Protection

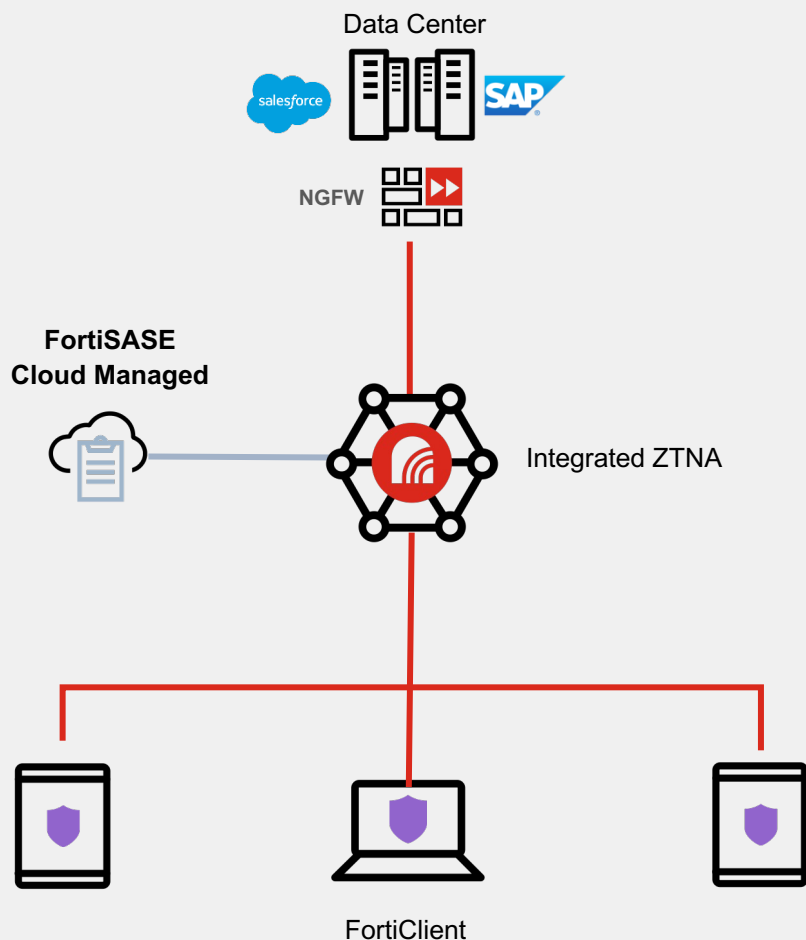
## LICENSE OFFERING

- User or Device-based licensing
- Stackable tiers from 25, 500, 2,000 or 10,000



# Use Case 2: Secure Private Access to Corporate Apps

No additional license required to enable natively available ZTNA in FortiSASE



## WHY it matters

Traditional VPN doesn't scale and complex to enable access to private applications

## HOW we solve it

- Provision and manage ZTNA automatically via FortiSASE management plane
- Allow explicit per-application access
- End point posture checks before traffic redirection

## BENEFITS

- Allow Secure access to corporate applications
- Automate & Speed ZTNA adoption

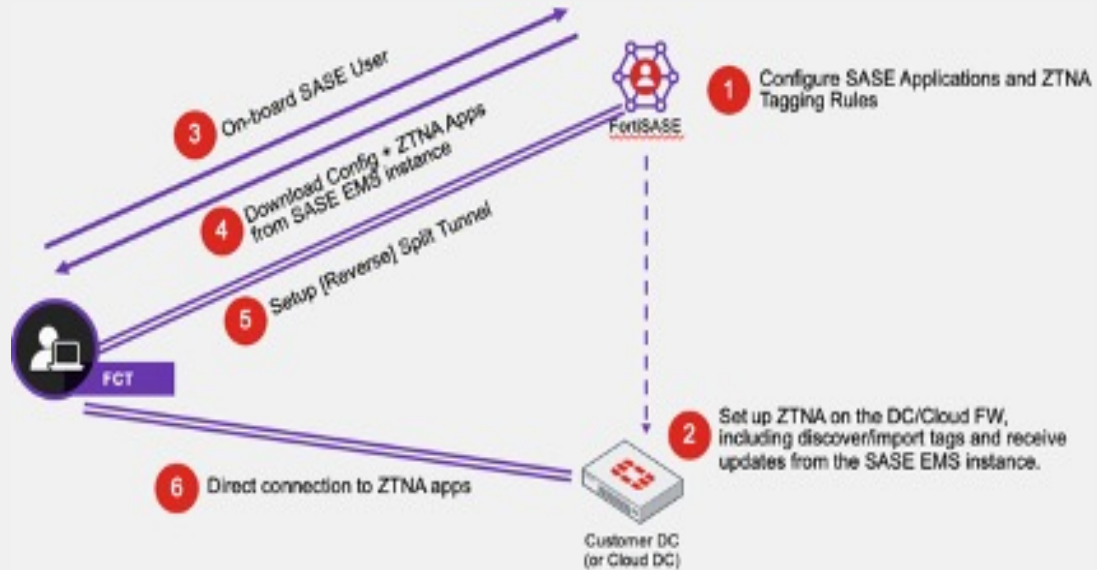
## LICENSE OFFERING

- No additional license required

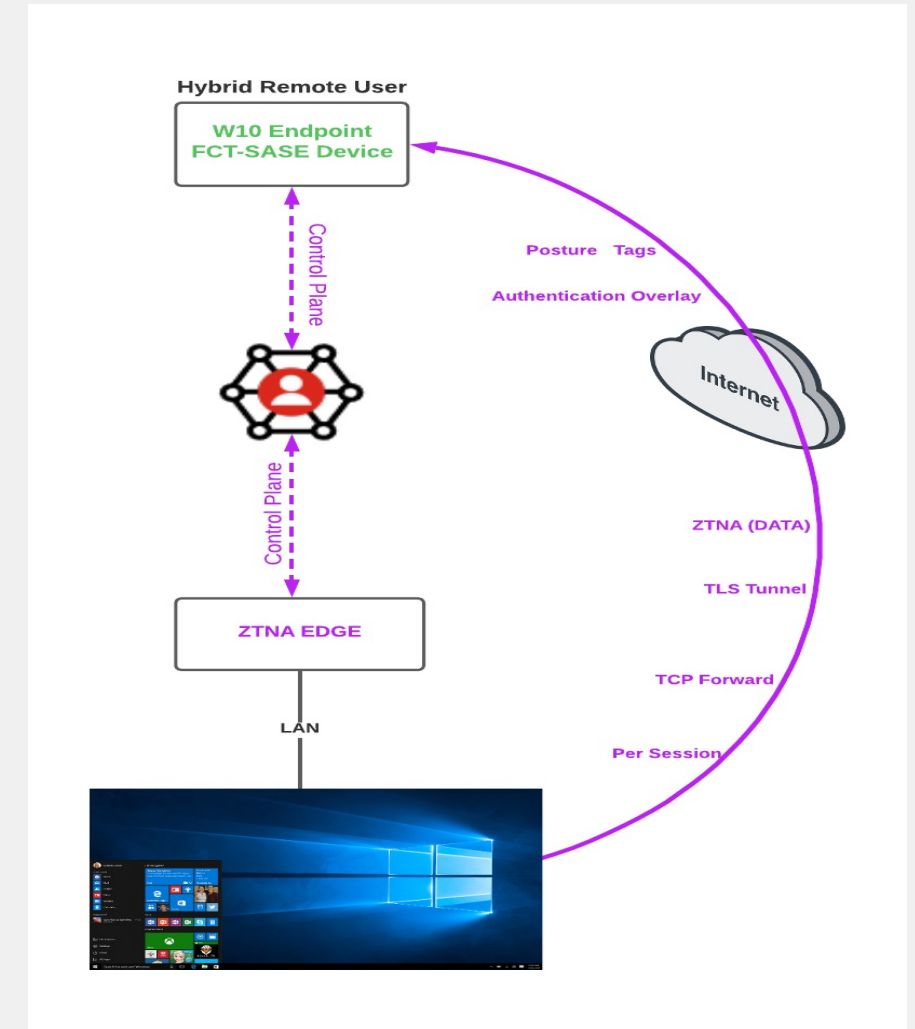


# FortiSASE Secure Private Access

## ZTNA

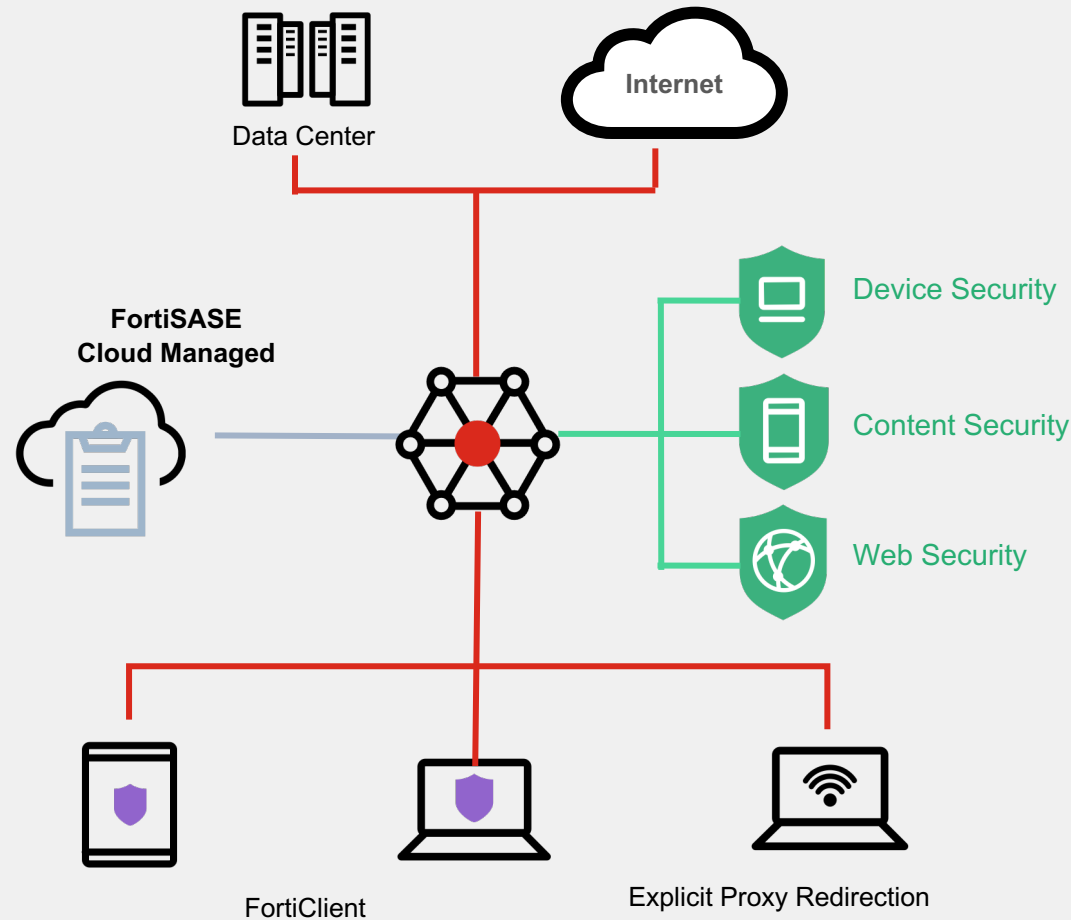


Private Access ZTNA



Private Access ZTNA – RDP Example

# Use Case 3: Simple Cloud-Based Management & Licensing



## WHY it matters

- Organizations shifting to OPEX from CAPEX model
- Complex operations demand simplified management

## HOW we solve it

- Simple cloud-based management without requiring the need to upgrade infrastructure


## BENEFITS

- Centralized management with same SASE portal
- No high CAPEX needed at every small branch
- Consistent security everywhere


## LICENSE OFFERING

- No additional license for management, troubleshooting, & logging


# FortiSASE Remote – Agent Based




itmanuser2




ZERO TRUST TELEMETRY




itmanuser2




ZERO TRUST TELEMETRY




REMOTE ACCESS




itmanuser2



ZERO TRUST TELEMETRY



REMOTE ACCESS



ZTNA CONNECTION RULES



MALWARE PROTECTION



SANDBOX DETECTION



VULNERABILITY SCAN




Notifications



Settings




About




## FortiClient - Connected


Zero Trust Fabric Agent



Managed by FortiClient Cloud

Status: ✔ Connected 

FortiSASE SIA (Secure Internet Access)



### AntiVirus Protection

Realtime-protection against file based malware & attack communication channels

Realtime Protection:	ON
Dynamic Threat Detection:	OFF
Block malicious websites:	ON
Threats Detected:	0

### FortiClient Cloud Sandbox

Behavior based advanced threat detection & zero-day threat protection by cloud sandbox.

Status: Connected

2	0	2	0
---	---	---	---

### Vulnerabilities

Helps detect and patch application vulnerabilities that can be exploited by known and unknown threats

Scan Schedule: No Scan Scheduled [\[Scan History\]](#)

Last Scan: Wed Apr 13 2022 13:07:08 GMT-0700 (Pacific Daylight Time)

[Scan Now](#)

### Vulnerabilities Detected

Total Vulnerabilities: 3

0 CRITICAL	3 HIGH	0 MEDIUM	0 LOW
---------------	-----------	-------------	----------

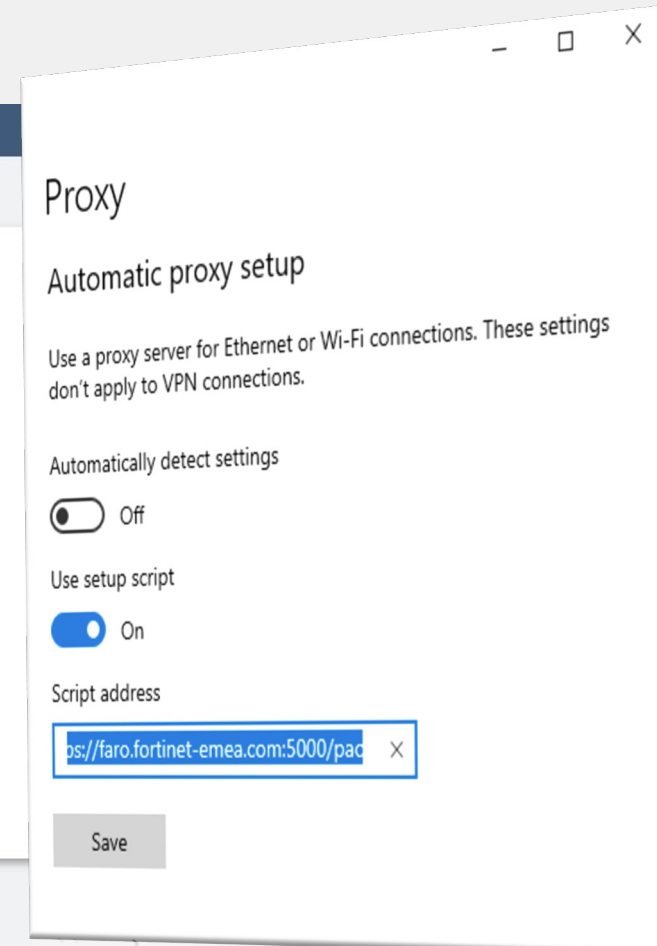
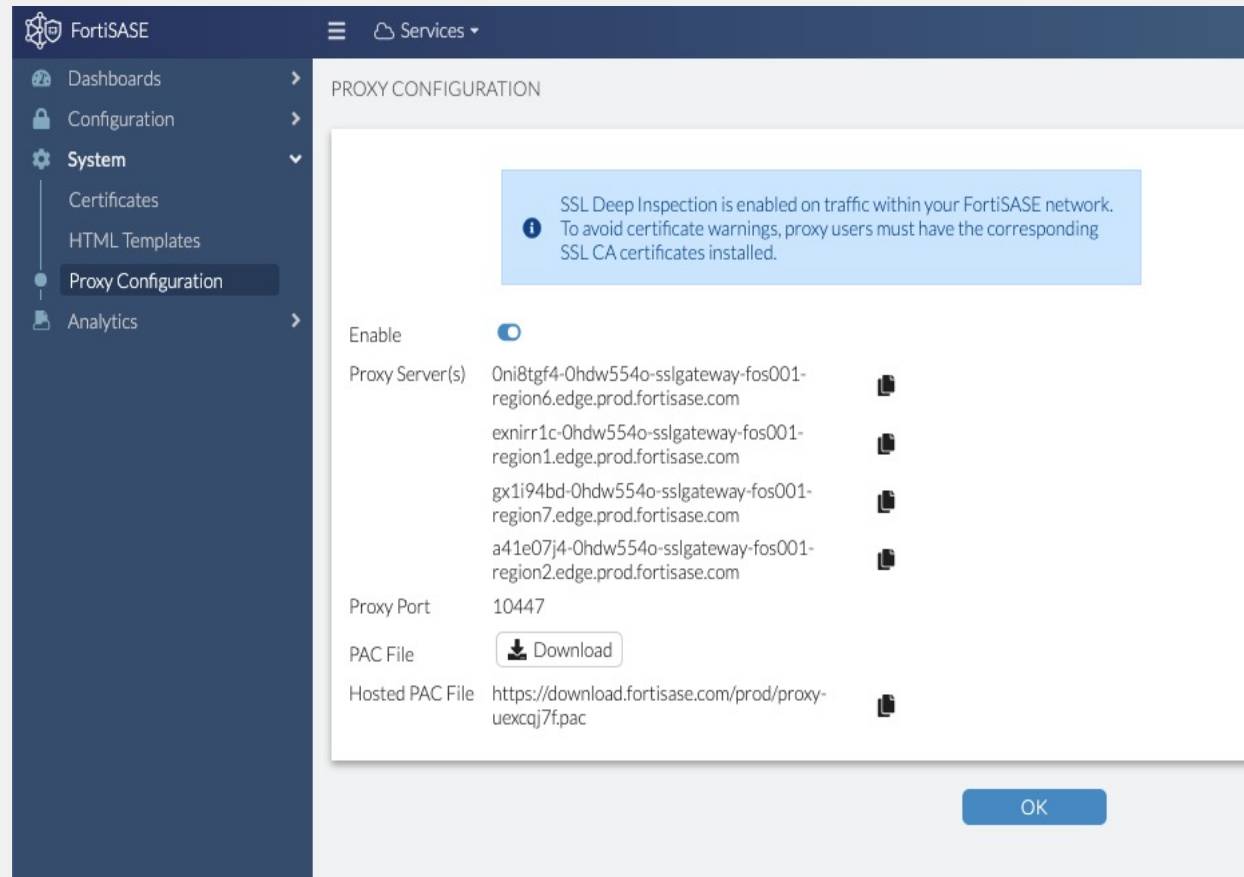
[Fix Now](#)

[illegible]

# Automated Proxy Deployment

## Simple Proxy Configuration

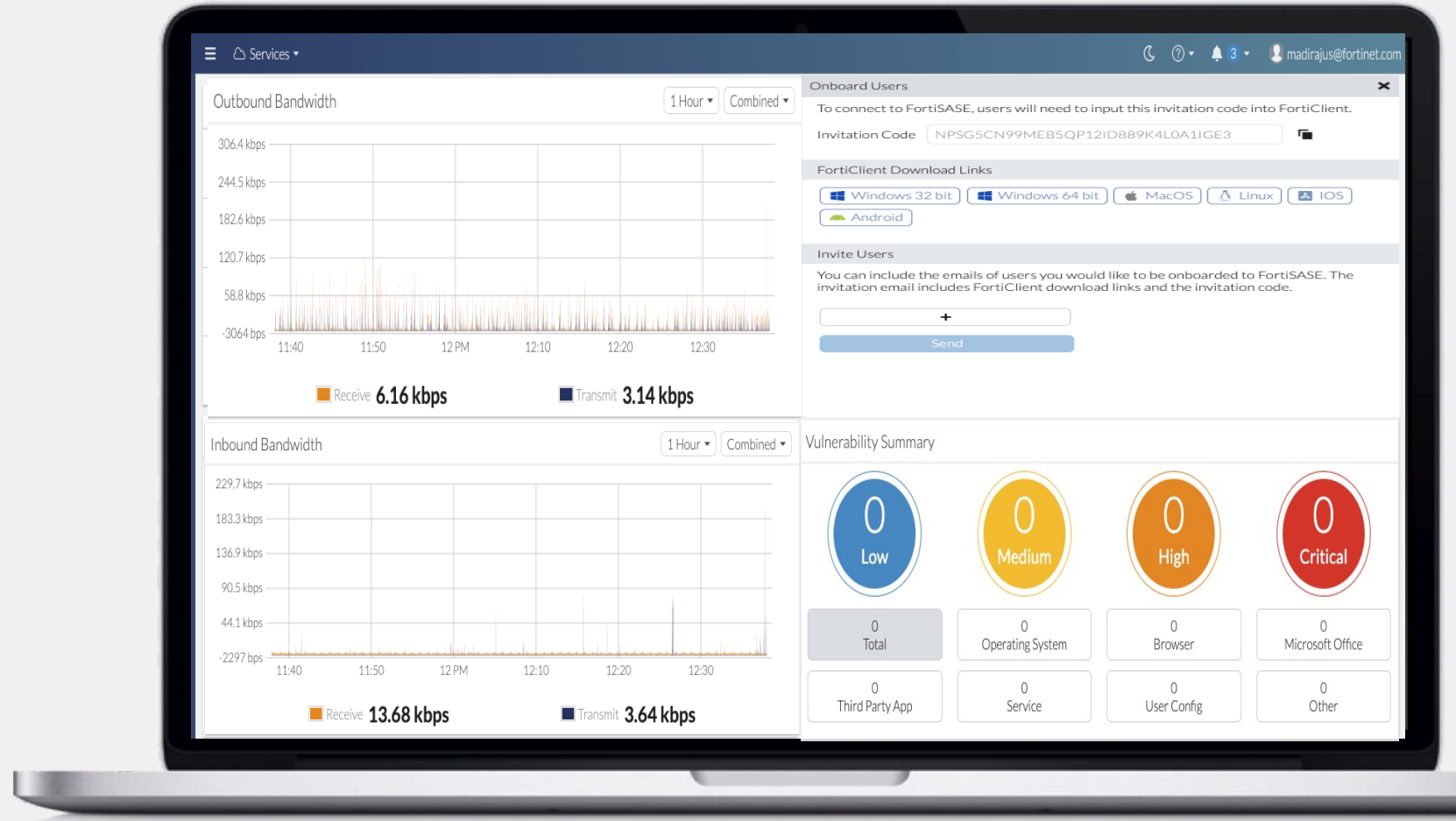
- Automatic Proxy Setup
- Certificate Management
- Customizable Block Pages



# Bird's-Eye View with Comprehensive Analytics

## Status Dashboard

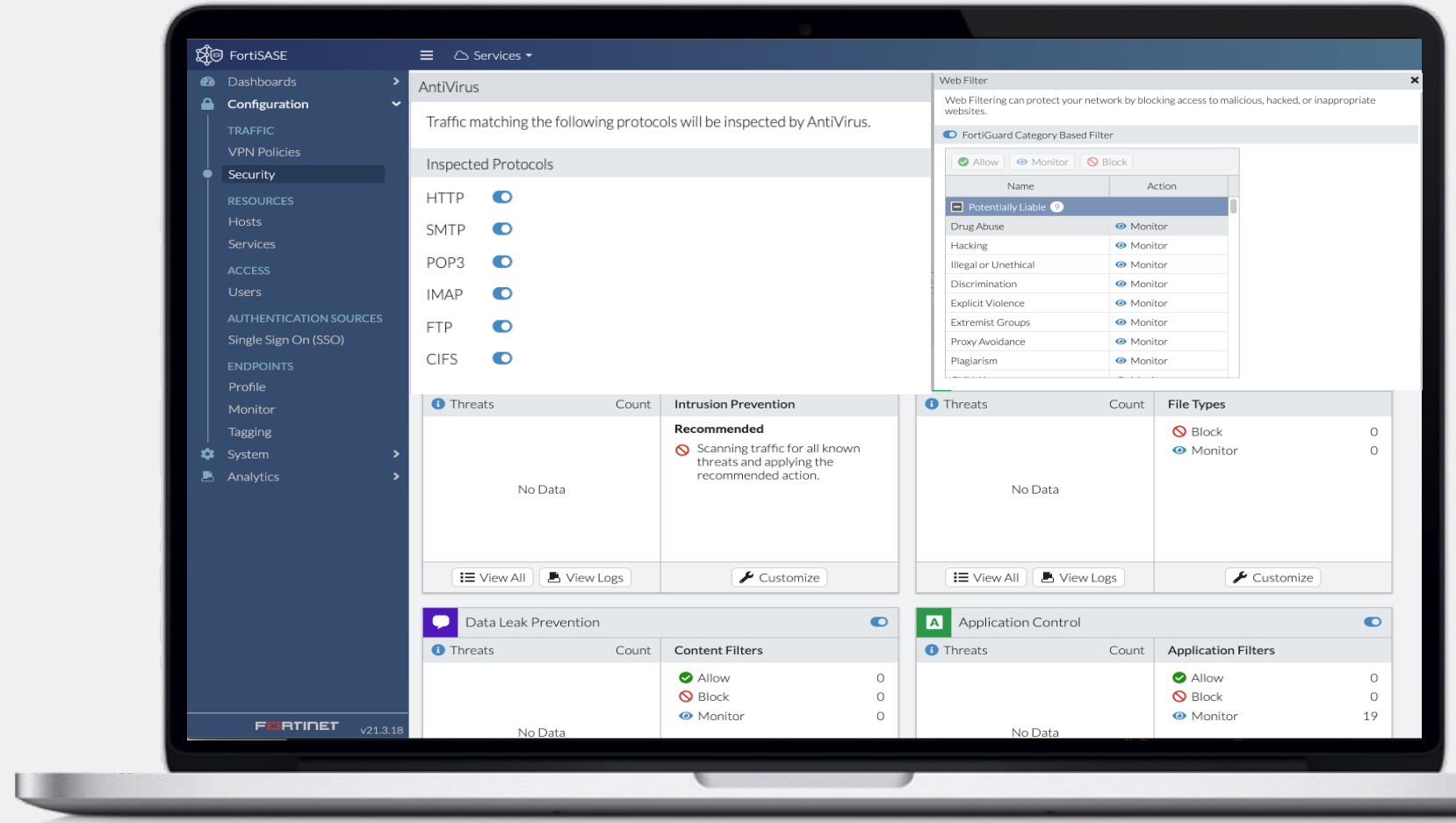
- Security Services Status with detailed Breakdown
- Simple Onboarding
- Managed Endpoints
- Inbound & Outbound bandwidth
- Vulnerability Summary



# Comprehensive Cloud-Delivered Secure Web Gateway

Widgets for :

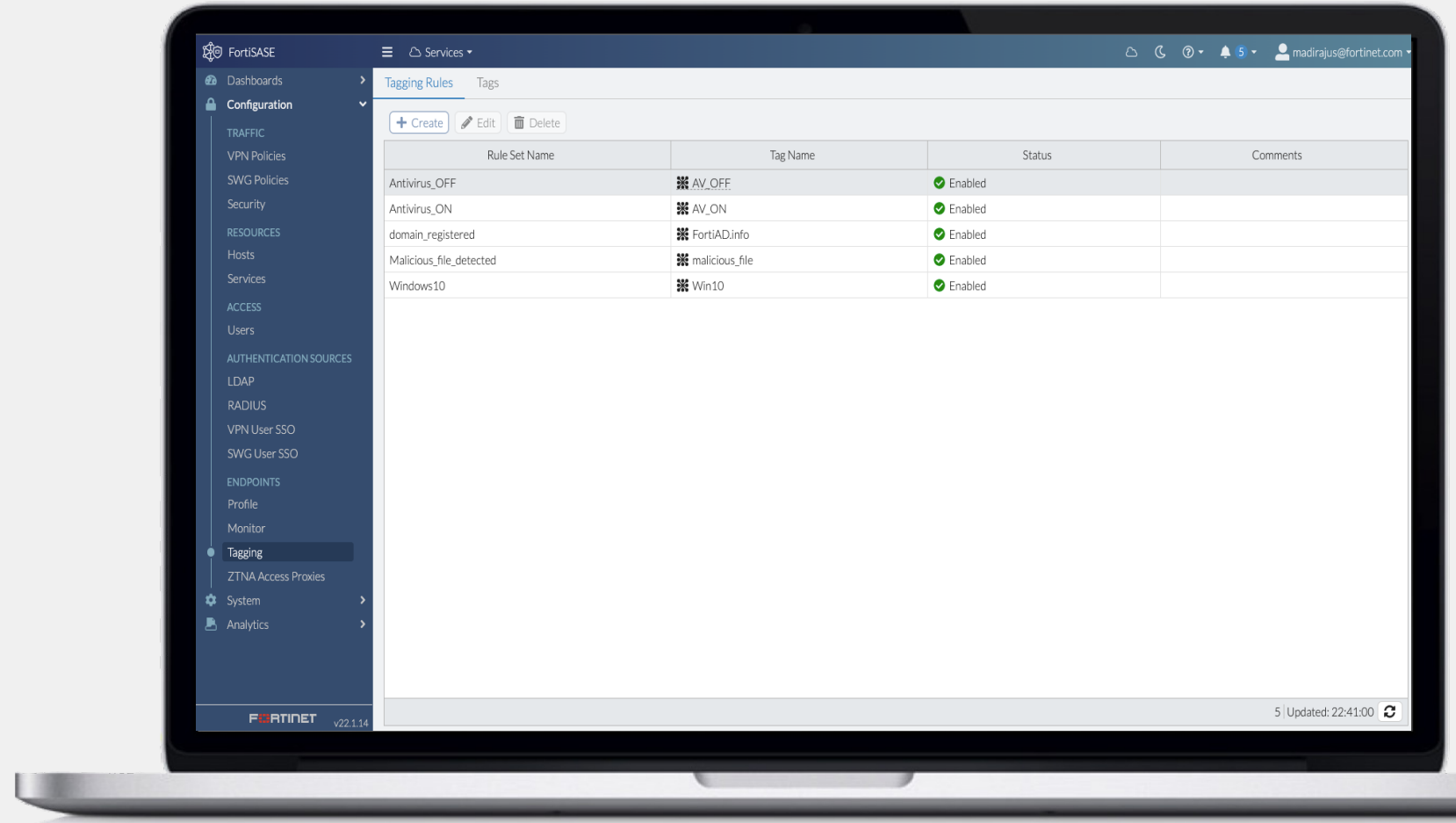
- Antivirus
  - Web Filtering IPS
  - File Filter
  - DLP
  - Application Control
  - SSL Inspection
- *Top Threats by Count*
- *Customizable Configuration*
- *Easy troubleshooting with detailed logging*



# FortiSASE with ZTNA for Secure Private Access

## Leveraging ZTNA Proxy:

- Configure SASE Applications & ZTNA Tagging Rules
- Setup ZTNA on FortiGate at Data center
- On-board SASE user
- Download ZTNA Apps and config to user agent
- Enable Secure private connection to corporate applications



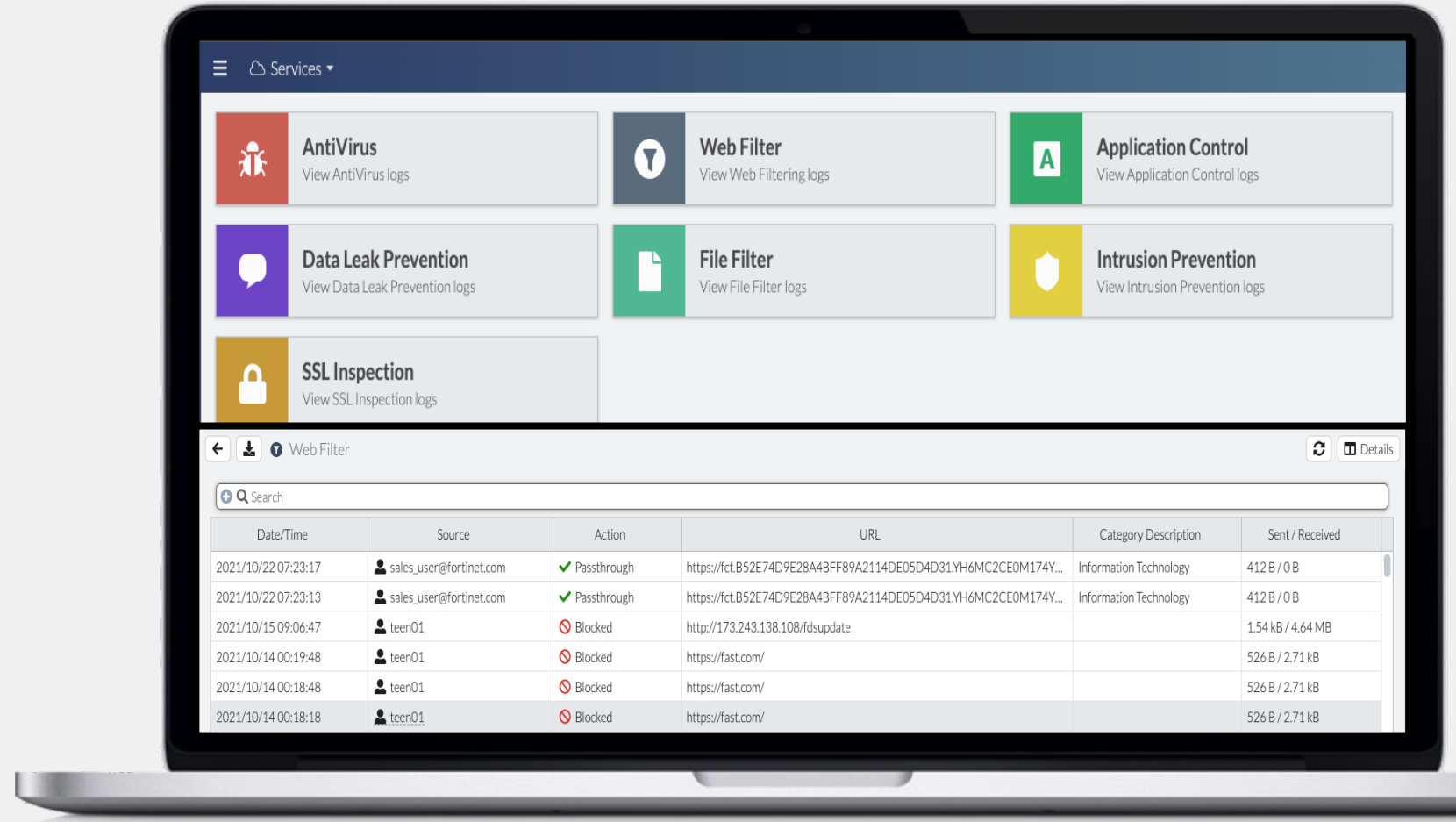
# Efficient Troubleshooting with Granular Logging & Events

- **Pre-Generated & On-Demand Reports**

- **Application :**
  - *Application Risk Control*
  - *Bandwidth Application Usage*
- **Security**
  - *Threat Report*
  - *Web Usage Report*
  - *VPN Report*

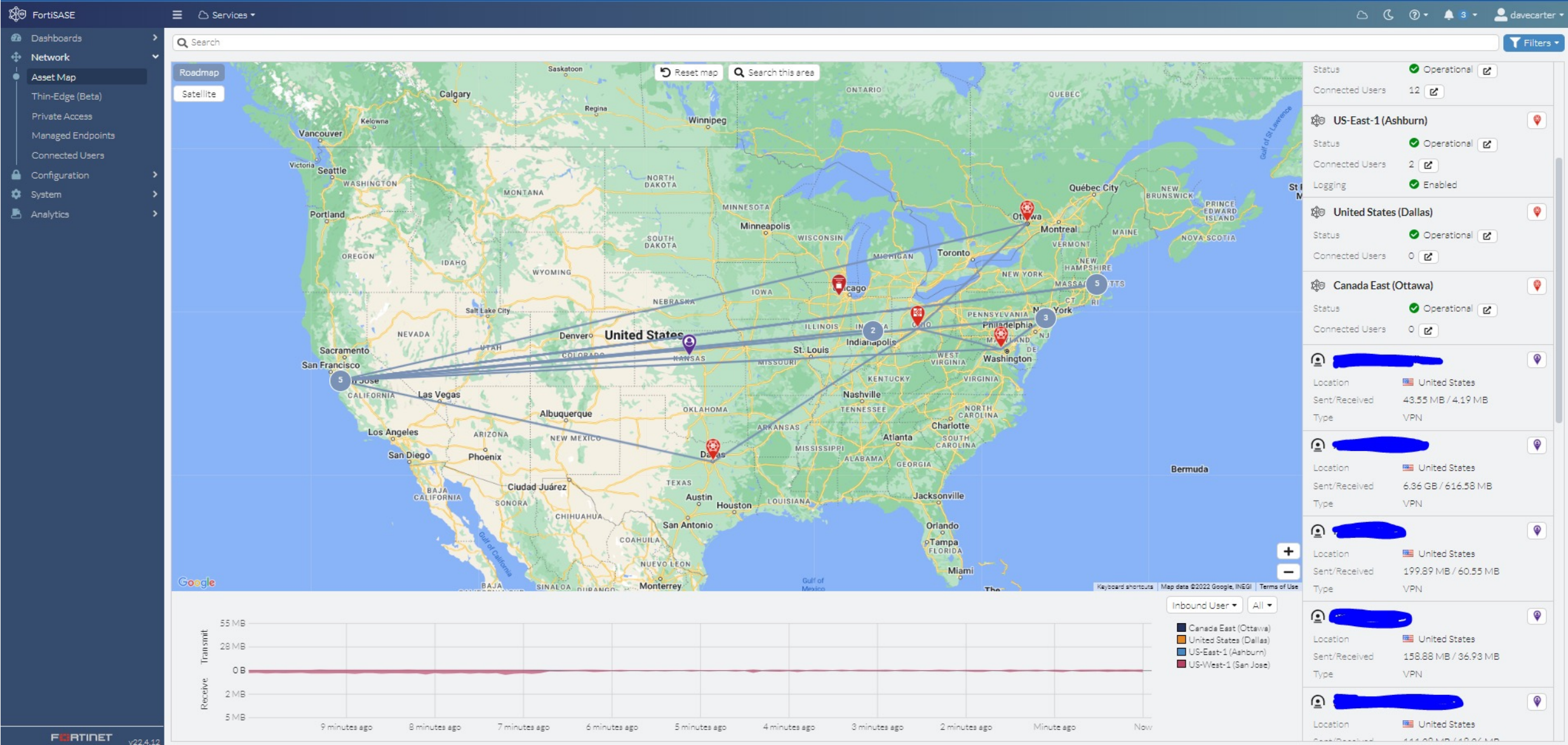
- **Logging & Events**

- **Security Logs**
- **User Events**
- **Endpoint Events**
- **VPN Events**





# Asset Map



# One SKU for Solution, Security Services & Cloud Management

## ORDER INFORMATION

REMOTE USERS	BANDS	FORTITRUST USER LICENSE	PACKS	USER LICENSE
FortiSASE Remote	100-499	FC2-10-EMS05-547-02-DD	25-pack	FC1-10-EMS05-553-01-DD
	500-1,999	FC3-10-EMS05-547-02-DD	500-pack	FC2-10-EMS05-553-01-DD
	2,000-9,999	FC4-10-EMS05-547-02-DD	2,000-pack	FC3-10-EMS05-553-01-DD
	10,000+	FC5-10-EMS05-547-02-DD	10,000 pack	FC4-10-EMS05-553-01-DD



# FAQ

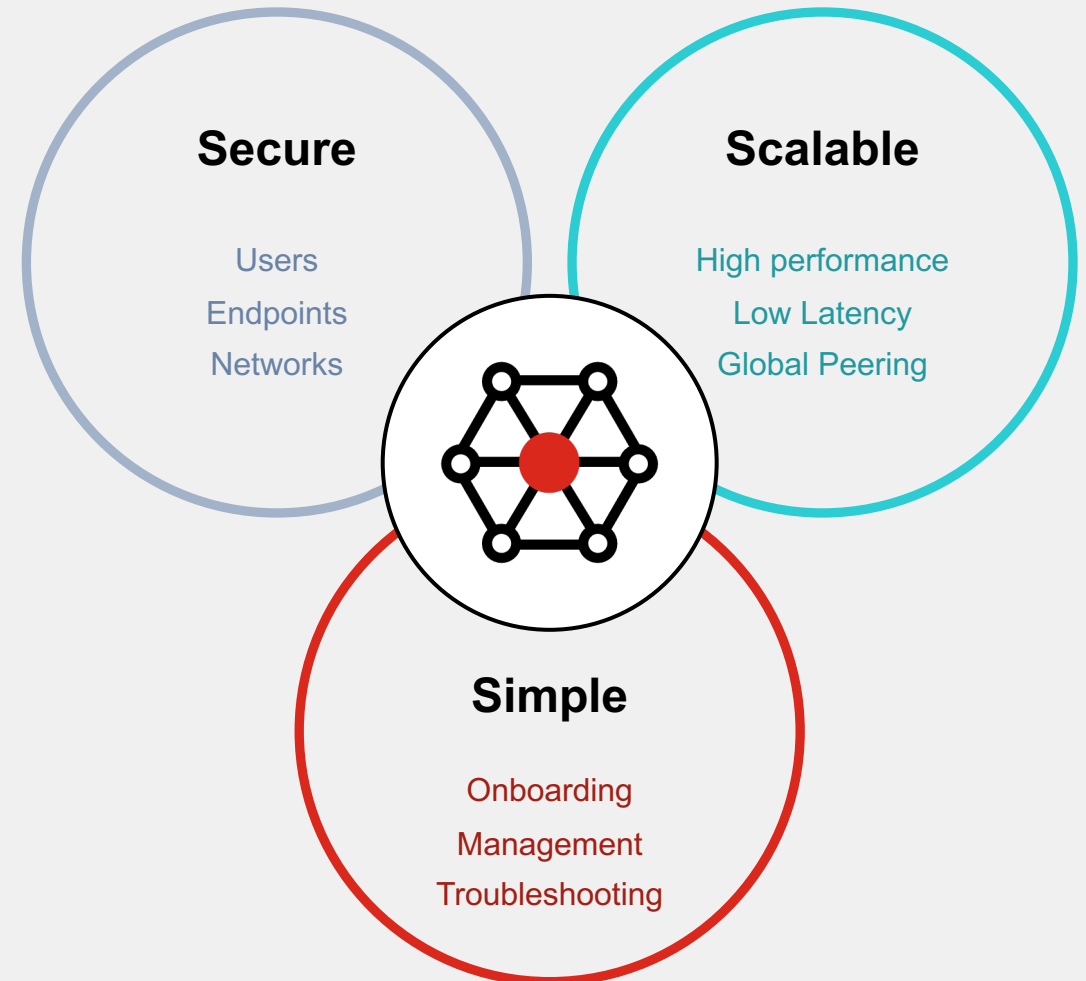
- **Q - How do I access Corporate Applications with FortiSASE?**
  - **A** - Use FortiSASE ZTNA which offers a direct connection to protected resources without requiring a persistent tunnel.
- **Q - Can my customer send logs to their SIEM?**
  - **A** - Yes, this is available and covered under the total bandwidth allotment per account.
- **Q - Can I mix and match user-based licenses?**
  - **A** - No, you cannot mix the FortiTrust user license (EMS05-547) with the user license (EMS05-553)
- **Q - What are the differences in protection provided when using the Agent and Agentless deployment models?**
  - **A** - Using the Agent based deployment model gives the end user ALL the SASE security components that include Cloud Based Inspection (DPI, AV, IPS, WebFilter, AppCtrl, DLP, BotNet C&C) PLUS the EPP features. Vulnerability Management, Sandbox, Malware Detection & Anti-Ransomware, and ZTNA. The Agentless deployment model ONLY provides the Cloud based Inspection.
- **Q - What are the different methods for an End Point to access the Internet?**
  - End Point Mode – FortiClient
  - SWG Mode – Explicit Proxy with PAC file
  - Thin Edge – FEX 200F Only – Max bandwidth 80Mbps



# FortiSASE: Key Takeaways

Fast, secure and scalable security for the hybrid workforce

- **Consistent Security Everywhere**
- **Integrated Broader Security Fabric**
- **Industry Leading Enterprise Security**



**FORTINET®**