FORTINET®

Unified SASE

Andrei Nitu-Ecxarcu

Systems Engineering Manager

Market Trends

Hybrid Workforce

84%

SOURCE 1:
2023 Forbes Remote Work Trends

Distributed Applications

125+

SOURCE 2:
2022 Gartner: Market Guide for SaaS Management Platforms

Active Vendor Consolidation

75%

SOURCE 3:
2022 Gartner CISO Survey and infographics

Zero Trust Mindset

Never Trust, Always Verify for resource protection

Grants network access only after identity is authenticated and authorized

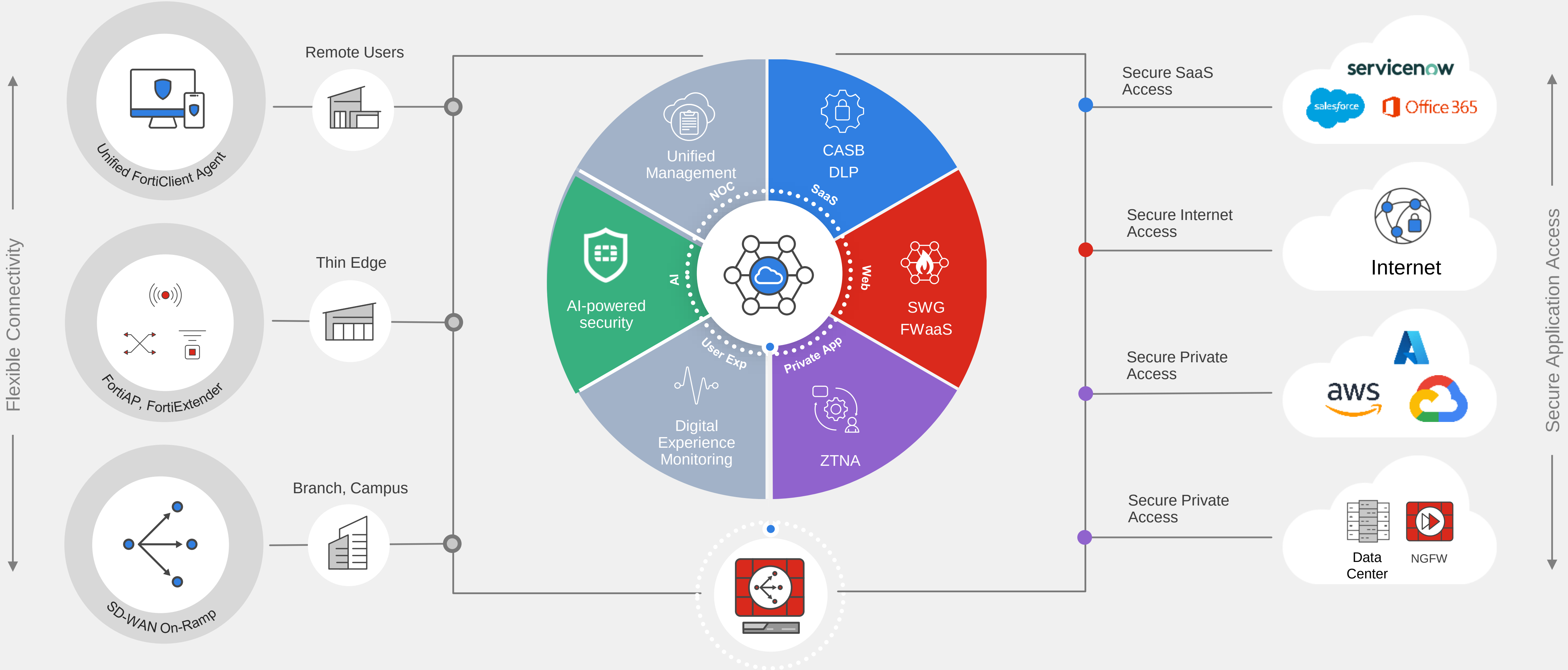
Limits network access only to necessary resources/applications

Continuously adjusts network access in near real time, based on device/user context

Fortinet SASE Solution

FortiSASE – Cloud Delivered SSE Solution

Rapid monthly release of new FortiSASE Innovations



Flexible Connectivity

Unified FortiClient Agent

Remote Users

FortiAP, FortiExtender

Thin Edge

SD-WAN On-Ramp

Branch, Campus

Unified Management

CASB
DLP

AI-powered security

SWG
FWaaS

Digital Experience Monitoring

ZTNA

NOC

SaaS

AI

Web

User Exp

Private App

Secure SD-WAN Network

Secure SaaS Access

Secure Internet Access

Secure Private Access

Secure Private Access

servicenow

salesforce

Office 365

Internet

aws

Data Center

NGFW

Secure Application Access

FortiSASE – One Console for Management and Visibility

FortiSASE Unified Management

Centralized Control

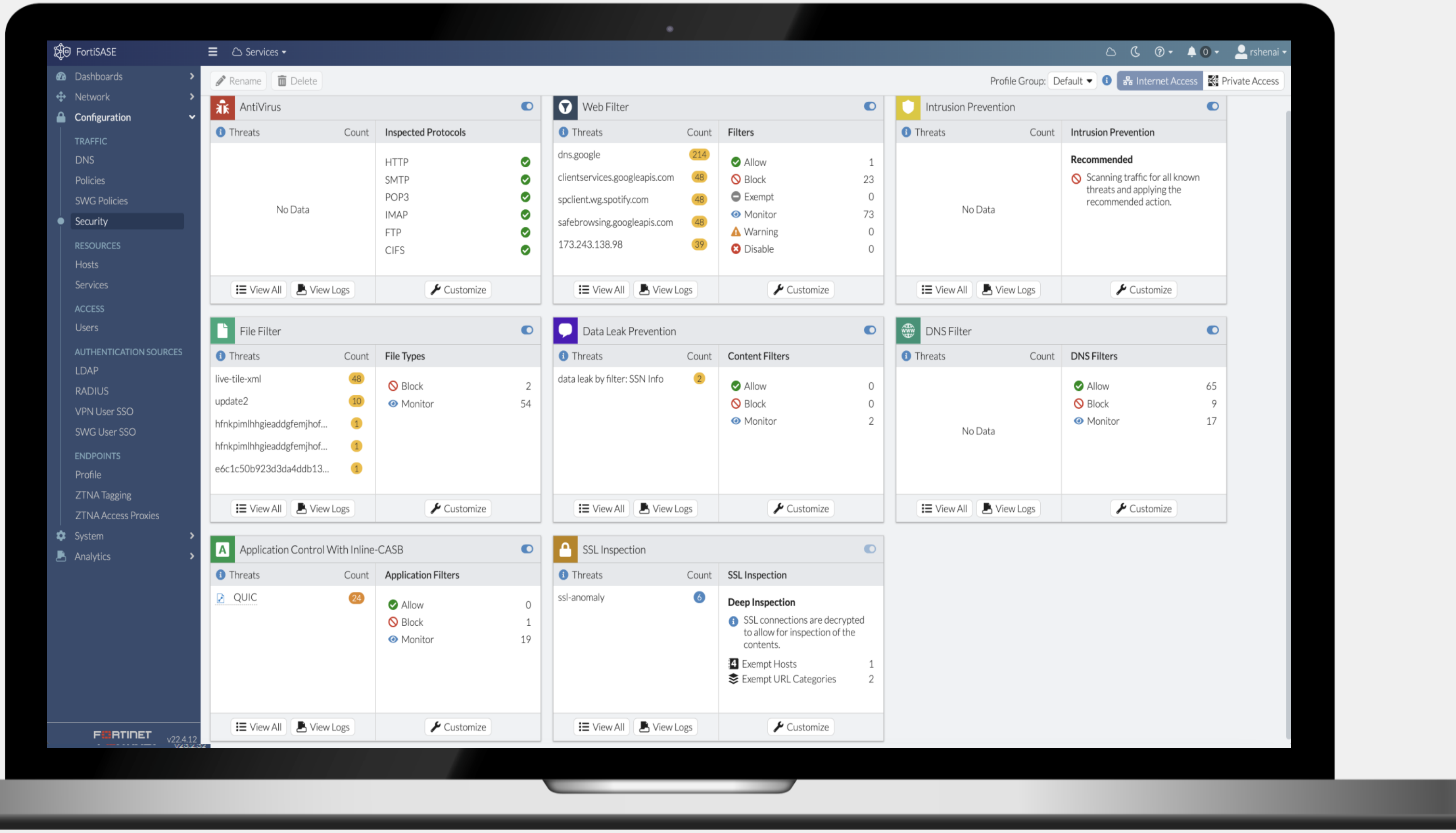
Control and configure all FortiSASE components
(SWG, FWaaS, ZTNA, CASB, DLP)

Single Console

Single pane for Internet and Private Access

Enhanced Visibility and Monitoring

Reporting, Analytics, Digital Experience Monitoring



AntiVirus

Threats	Count
No Data	

Inspected Protocols	
HTTP	✓
SMTP	✓
POP3	✓
IMAP	✓
FTP	✓
CIFS	✓

Web Filter

Threats	Count
dns.google	214
clientservices.googleapis.com	48
spclient.wg.spotify.com	48
safebrowsing.googleapis.com	48
173.243.138.98	39

Filters	
Allow	1
Block	23
Exempt	0
Monitor	73
Warning	0
Disable	0

Intrusion Prevention

Threats	Count
No Data	

Intrusion Prevention

Recommended

Scanning traffic for all known threats and applying the recommended action.

File Filter

Threats	Count
live-tile-xml	48
update2	10
hfnkpimlhhgieaddgfemjhof...	1
hfnkpimlhhgieaddgfemjhof...	1
e6c1c50b923d3da4ddb13...	1

File Types	
Block	2
Monitor	54

Data Leak Prevention

Threats	Count
data leak by filter: SSN Info	2

Content Filters	
Allow	0
Block	0
Monitor	2

DNS Filter

Threats	Count
No Data	

DNS Filters	
Allow	65
Block	9
Monitor	17

Application Control With Inline-CASB

Threats	Count
QUIC	24

Application Filters	
Allow	0
Block	1
Monitor	19

SSL Inspection

Threats	Count
ssl-anomaly	6

SSL Inspection

Deep Inspection

SSL connections are decrypted to allow for inspection of the contents.

Exempt Hosts	1
Exempt URL Categories	2

FortiSASE – One Agent for Simplified Deployment

Converge Legacy Agents into a Single Solution

FortiSASE Unified agent

Simplified Deployment

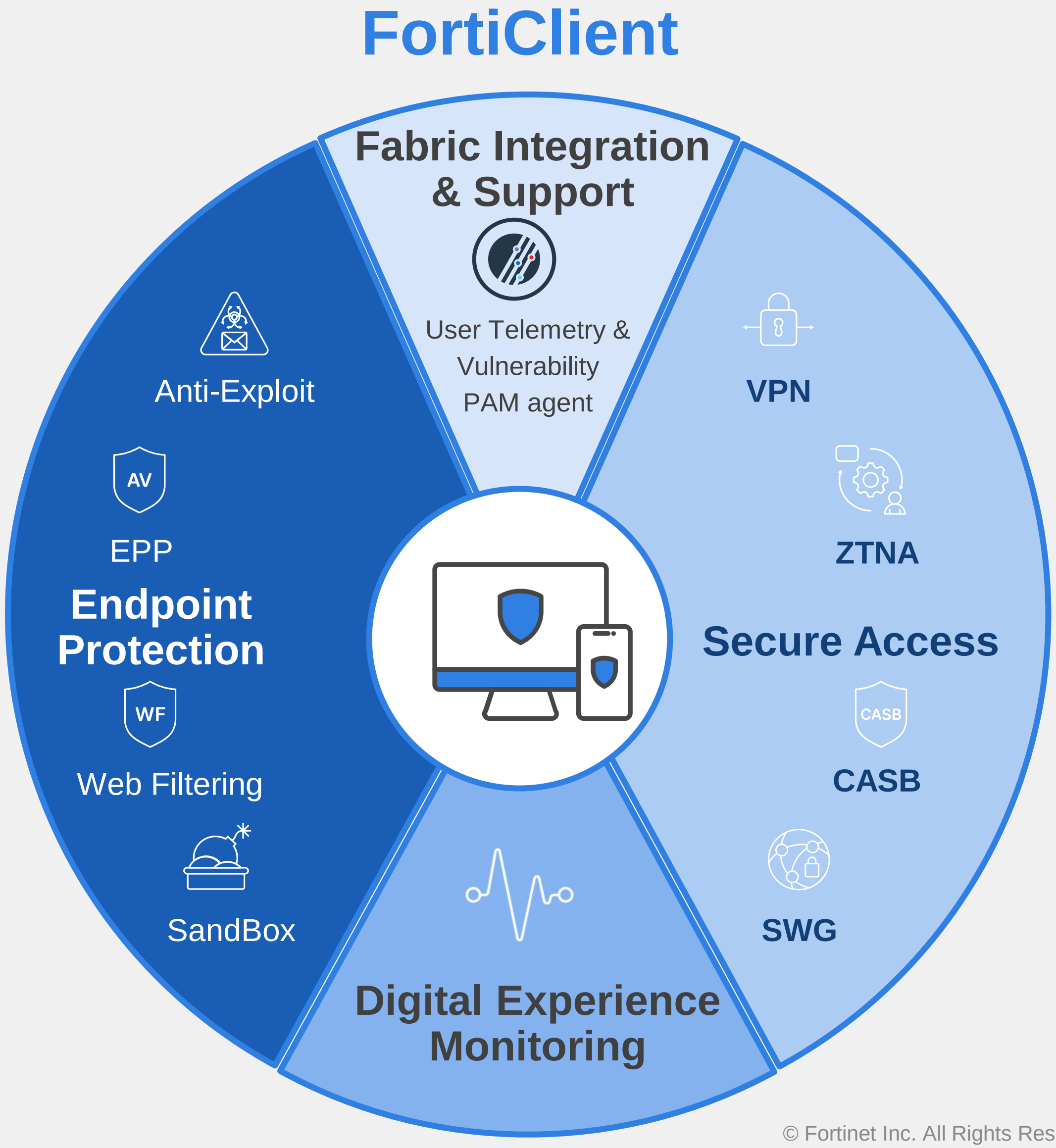
No need to install and update separate agents for EPP, SSE, DEM

Comprehensive Endpoint Protection

Full protection of endpoint with antivirus

Enhanced Visibility and Control

Telemetry, Digital Experience Monitoring, endpoint activities


FortiClient

Fabric Integration & Support

User Telemetry & Vulnerability PAM agent

Endpoint Protection

Anti-Exploit

EPP

Web Filtering

SandBox

Secure Access

VPN

ZTNA

CASB

SWG

Digital Experience Monitoring

FortiSASE - Flexible security with Thin Edge deployments

FortiSASE Thin Edge Security

Secure Smaller Locations

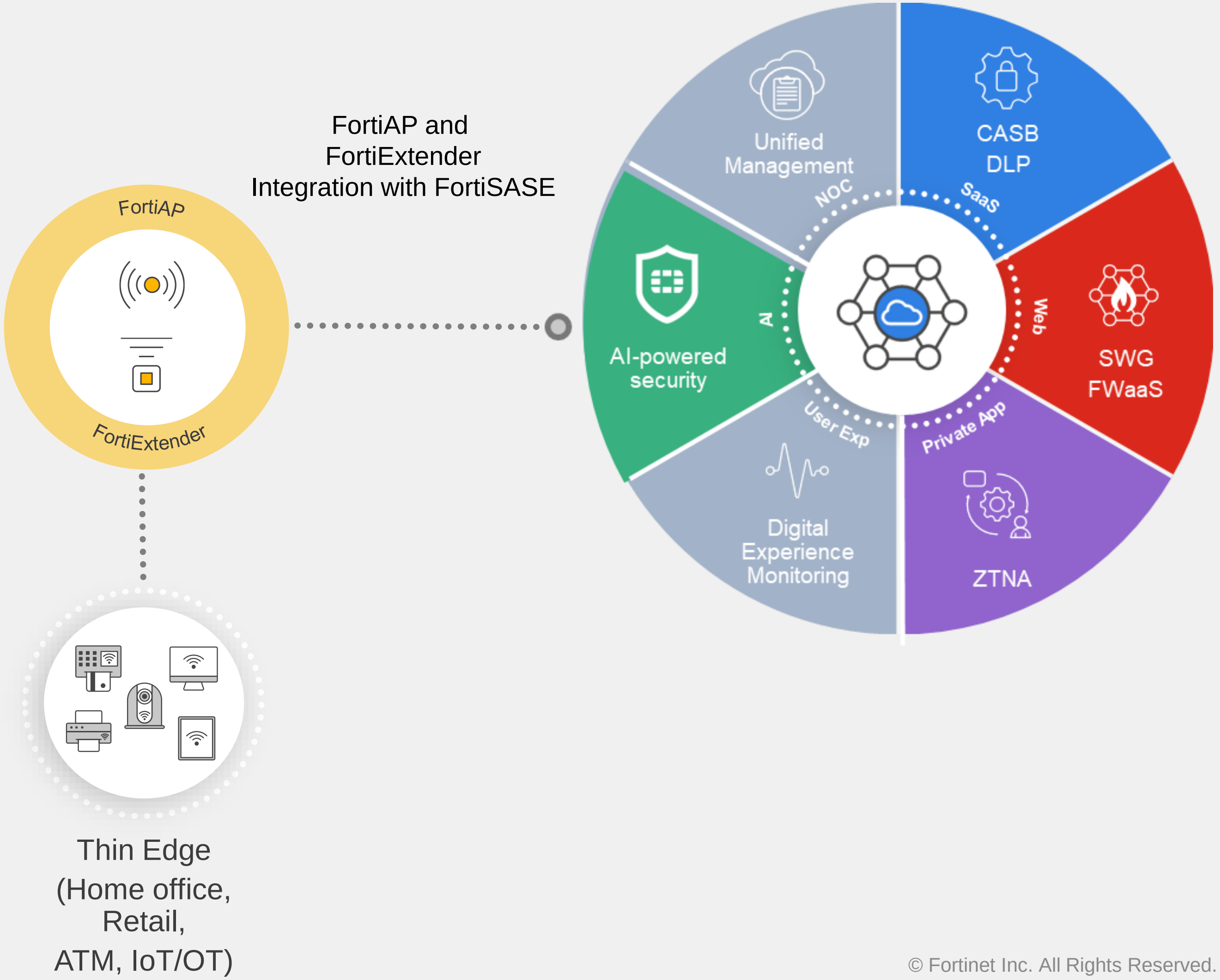
Secure small locations, pop-up locations or home offices without the need of a firewall

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



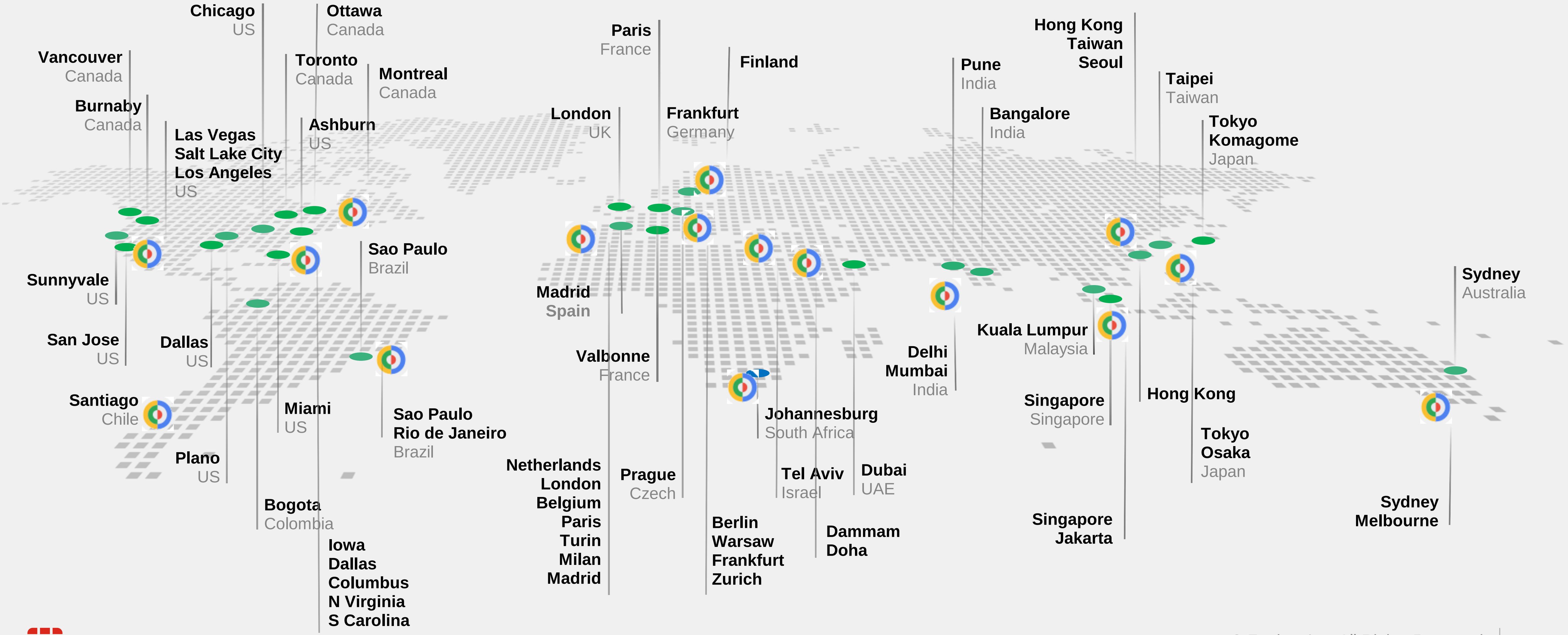
Scalable Cloud Network for Best User Experience

Global Coverage

140+ Cloud Locations

Security As a Service

Low Latency, High SLA



Vancouver
Canada

Burnaby
Canada

Chicago
US

Las Vegas
Salt Lake City
Los Angeles
US

Toronto
Canada

Ottawa
Canada

Ashburn
US

Montreal
Canada

Sunnyvale
US

San Jose
US

Dallas
US

Santiago
Chile

Plano
US

Miami
US

Bogota
Colombia

Iowa
Dallas
Columbus
N Virginia
S Carolina

Sao Paulo
Brazil

Sao Paulo
Rio de Janeiro
Brazil

Paris
France

London
UK

Frankfurt
Germany

Finland

Madrid
Spain

Valbonne
France

Netherlands
London
Belgium
Paris
Turin
Milan
Madrid

Prague
Czech

Berlin
Warsaw
Frankfurt
Zurich

Johannesburg
South Africa

Tel Aviv
Israel

Dubai
UAE

Dammam
Doha

Pune
India

Bangalore
India

Delhi
Mumbai
India

Hong Kong
Taiwan
Seoul

Taipei
Taiwan

Tokyo
Komagome
Japan

Kuala Lumpur
Malaysia

Singapore
Singapore

Singapore
Jakarta

Hong Kong

Tokyo
Osaka
Japan

Sydney
Australia

Sydney
Melbourne

Use cases

Secure Internet Access

For Remote Users, Thin Edge and Branch Locations

Safe browsing from anywhere

Malware & Ransomware prevention

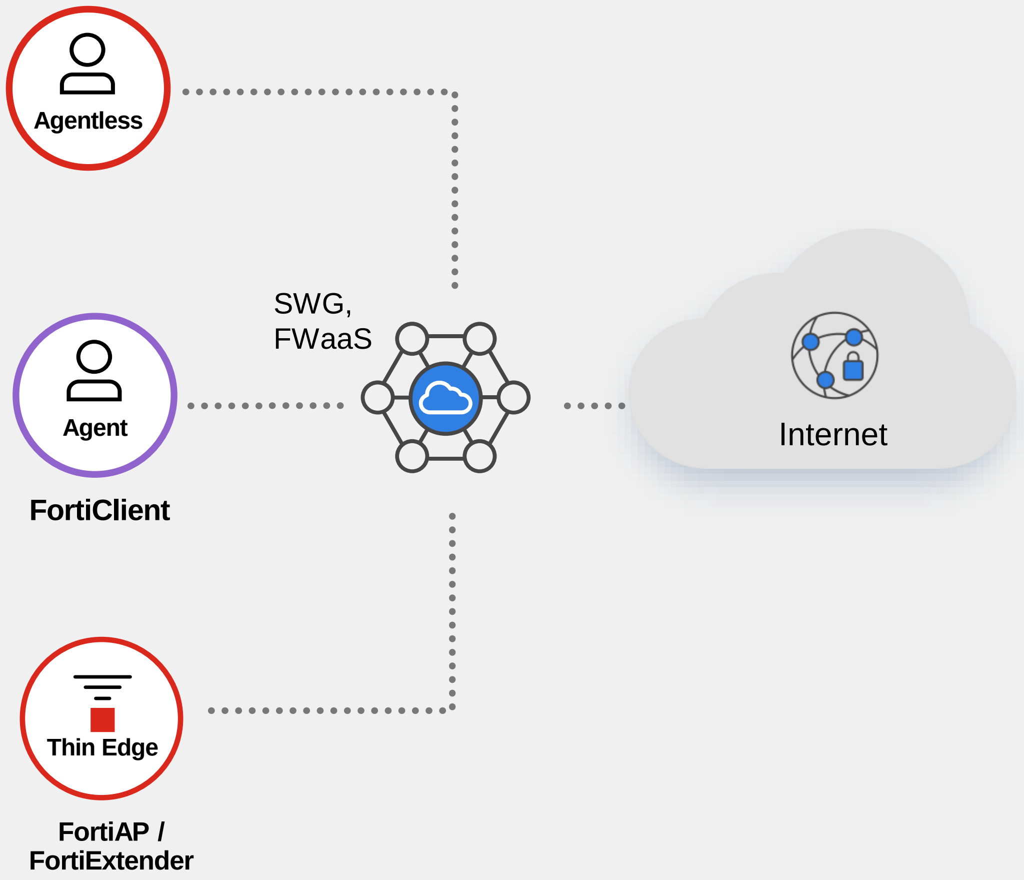
Prevent threats with cloud-based Firewall, IPS, Web Filtering, Anti-virus, DNS and File Filtering, Sandbox

Deep SSL Inspection of end-user activity

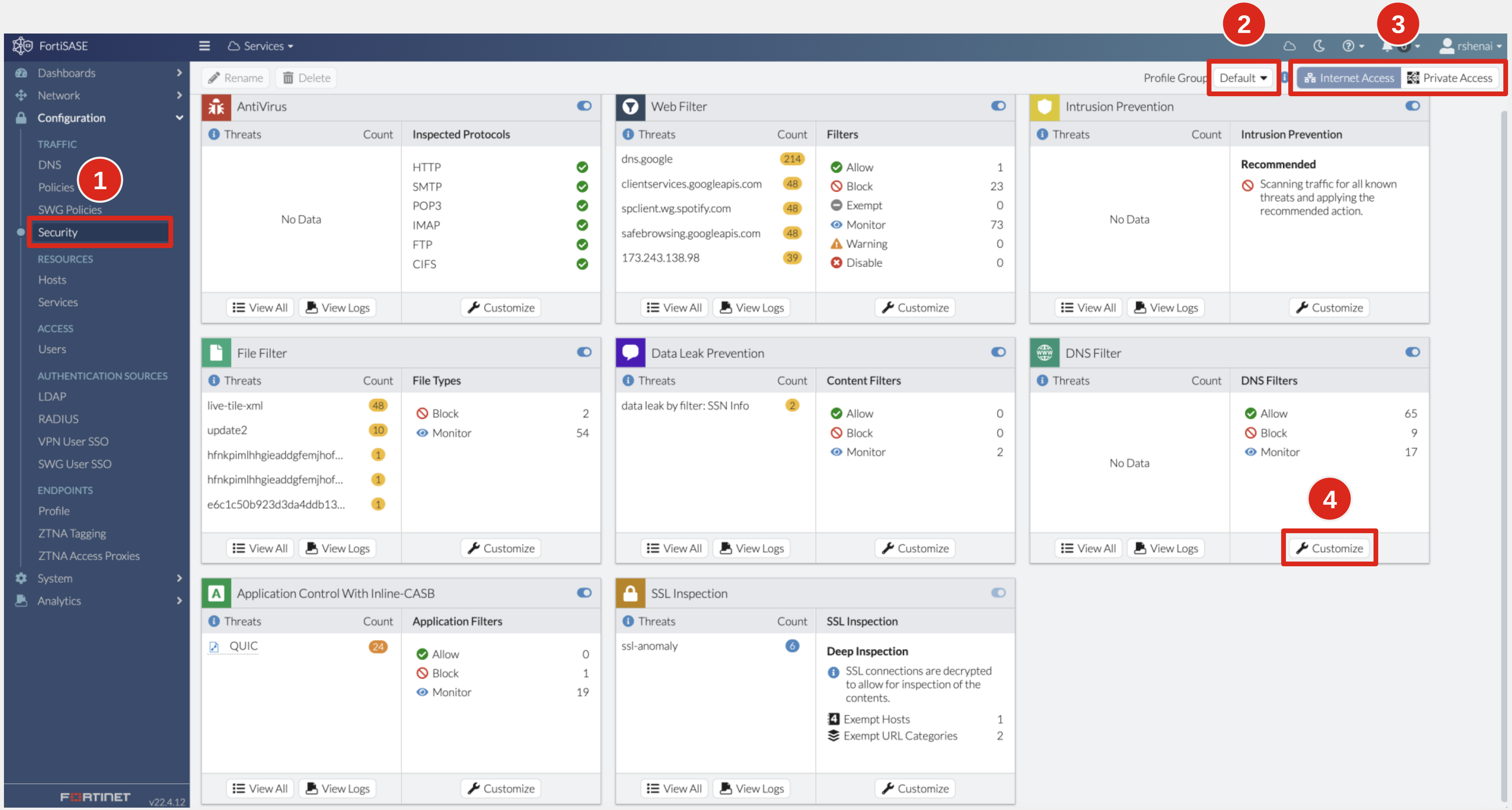
Deep inspection of web activity for threats, even when using secured HTTPS access

AI Powered Security Services

Best in class security efficacy and zero-day threat protection with AI powered FortiGuard Security Services



Secure Internet Access – Threat Protection



AntiVirus

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

Web Filter

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

Intrusion Prevention

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

File Filter

Threats	Count	File Types	
live-tile-xml	48	Block	2
update2	10	Monitor	54
hfnkpimlhhgieaddgfemjhof...	1		
hfnkpimlhhgieaddgfemjhof...	1		
e6c1c50b923d3da4ddb13...	1		

Data Leak Prevention

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

DNS Filter

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

Application Control With Inline-CASB

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

SSL Inspection

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

Secure Private Access

With ZTNA and SD-WAN integration

Secure corporate app access

Secure Cloud & datacenter app access

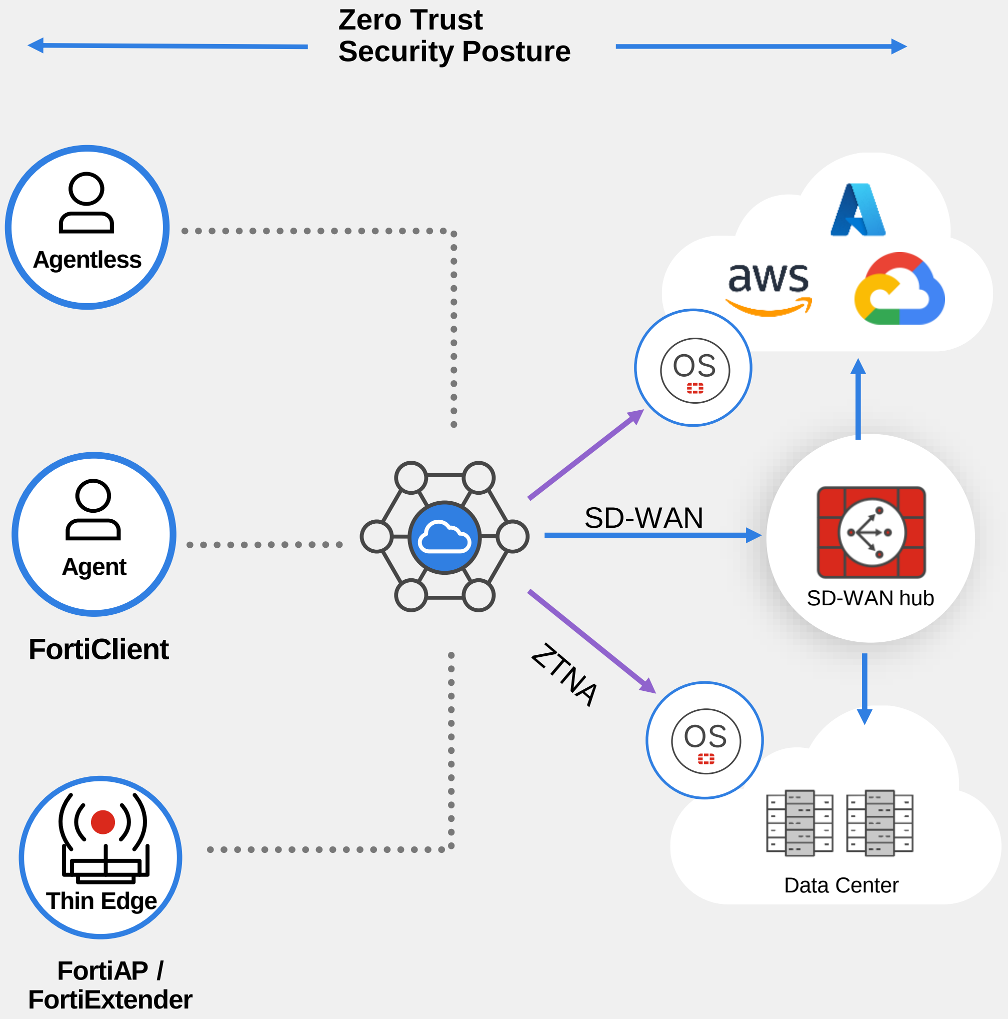
Secure anywhere access to corporate applications in datacenter and cloud with deep security inspection

Universal Zero-trust Network Access

User identity and device context-based zero-trust access to explicit applications from remote or on-prem location

SD-WAN integration

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



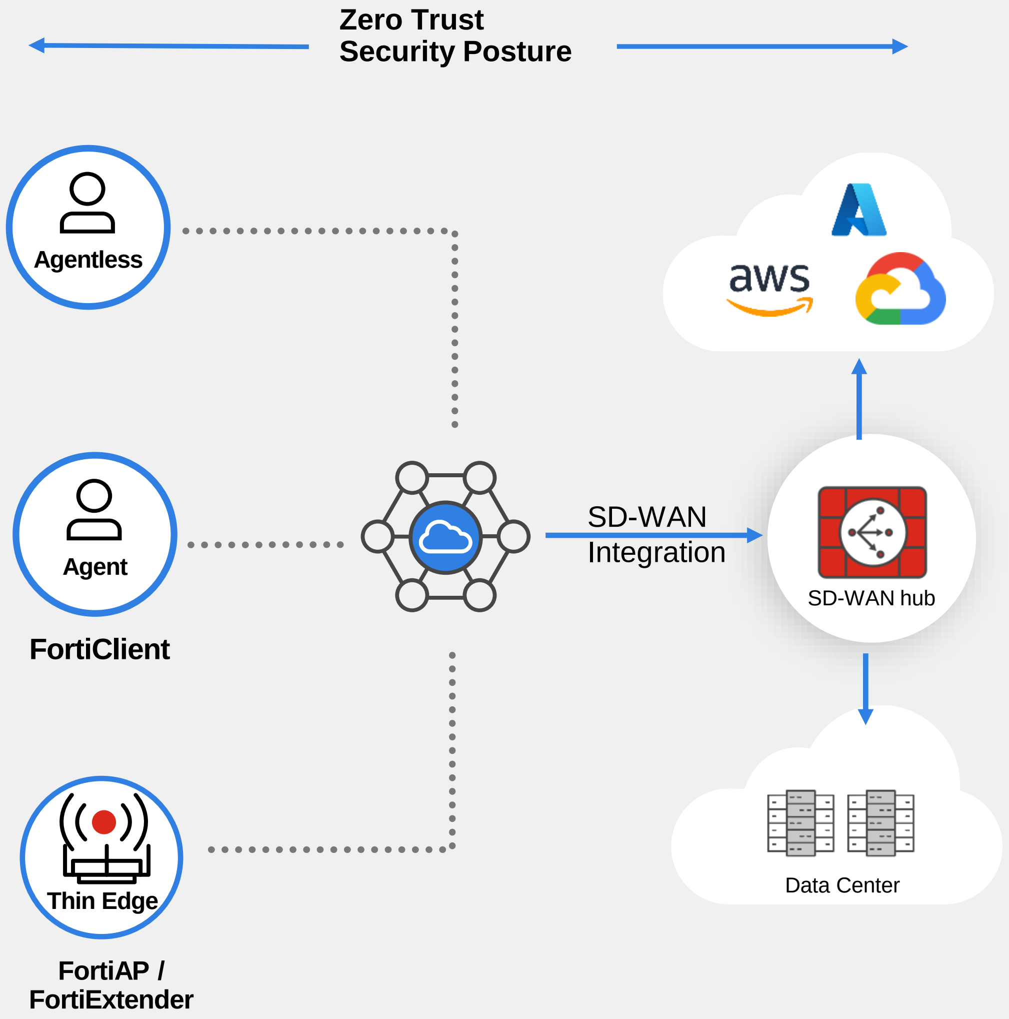
Secure Private Access with SD-WAN Integration

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)

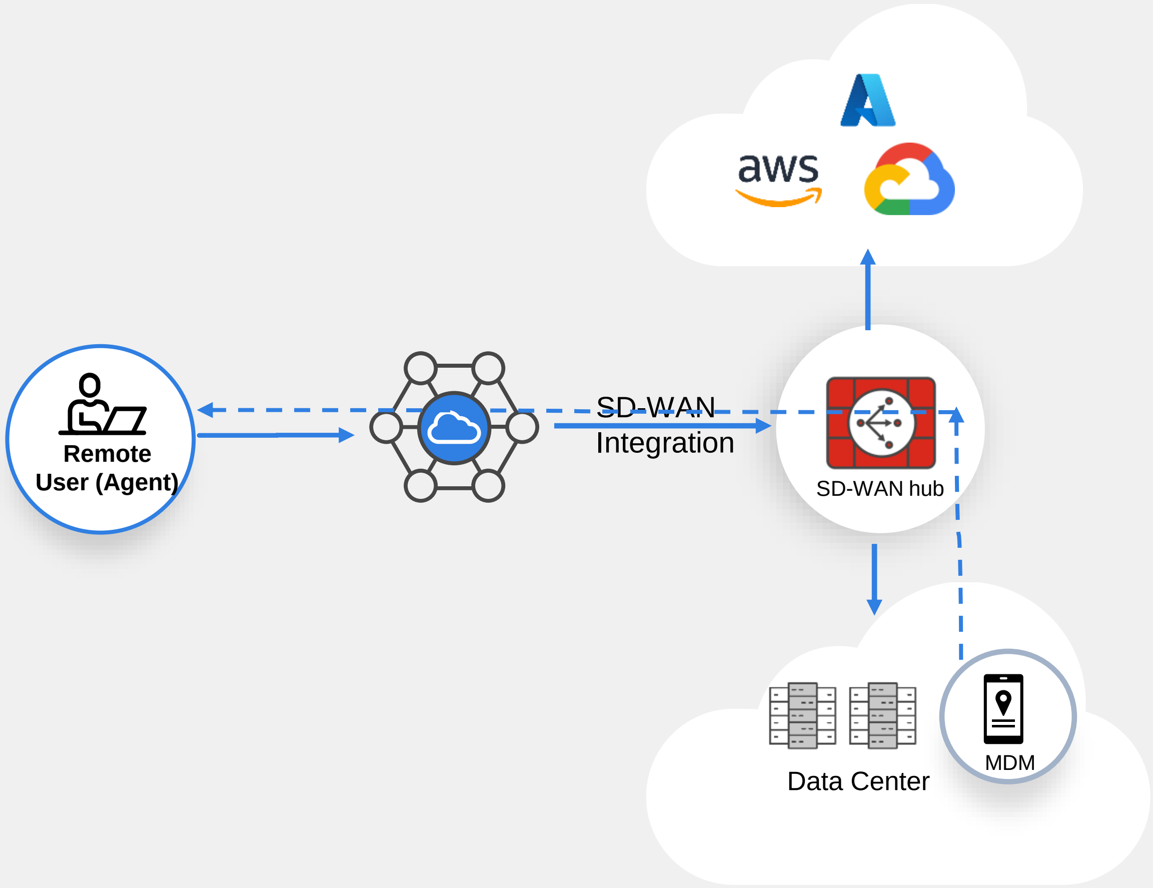


Secure Private Access - What's New

Bi-directional Traffic Support for Secure Private Access with SD-WAN Integration

Server to Client Traffic Support

- Allow trusted traffic from applications on the SD-WAN network to securely connect to remote user devices (e.g., MDM, Remote Desktop)
- Requires environment to have the remote VPN user identification feature enabled



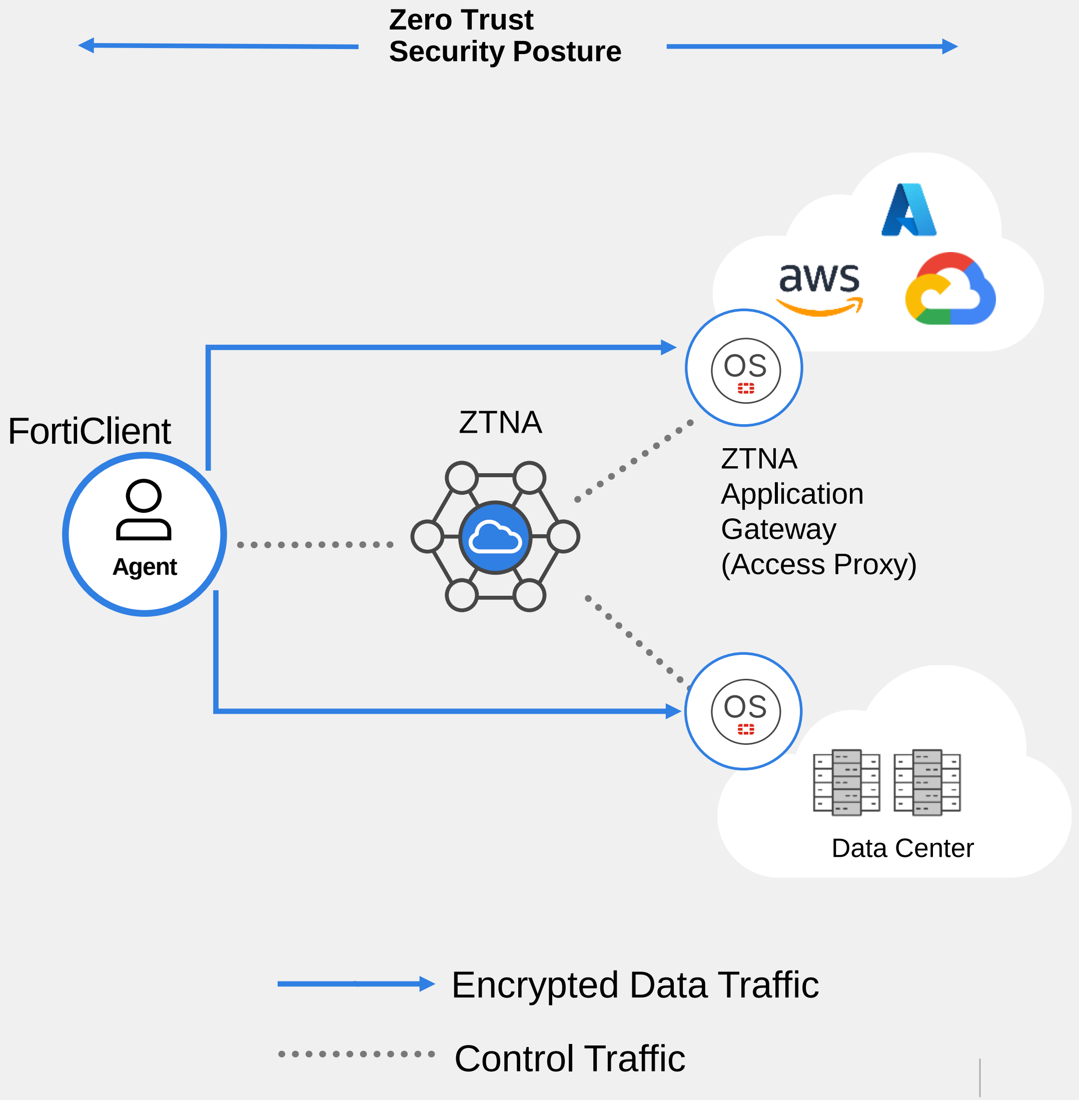
Secure Private Access with ZTNA

FortiSASE ZTNA Support

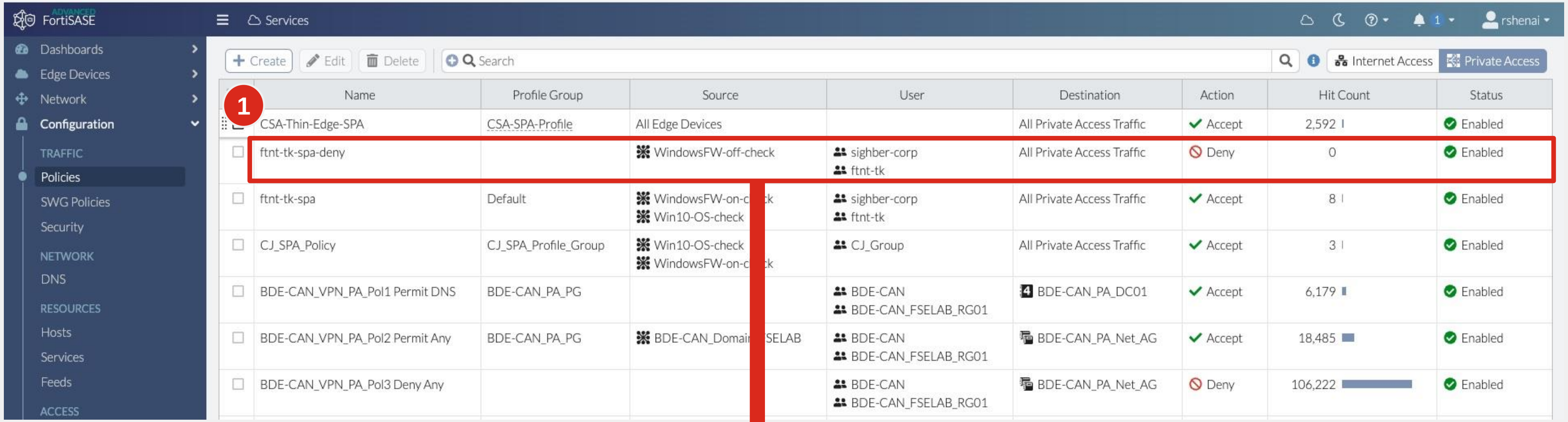
Zero-trust access based on **user/device identity** and **device posture**

Granular and **explicit application access** control per-session

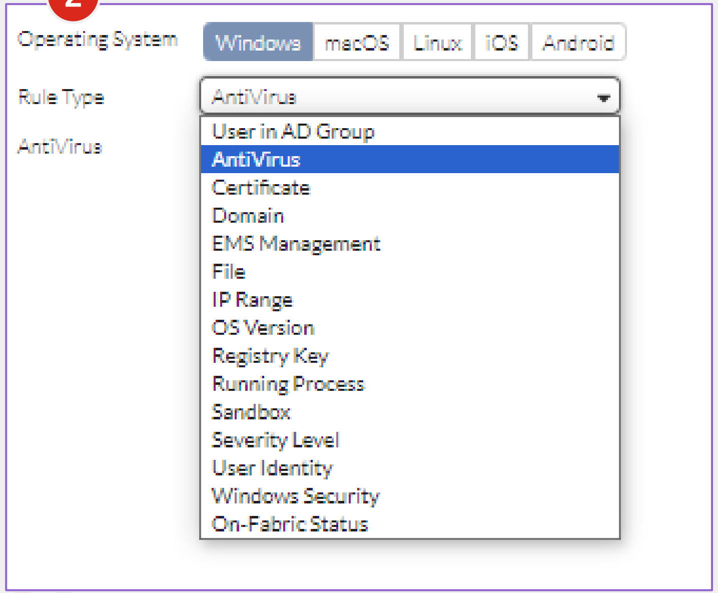
Continuous device posture re-assessment (every 60 seconds)



Zero Trust security for secure application access



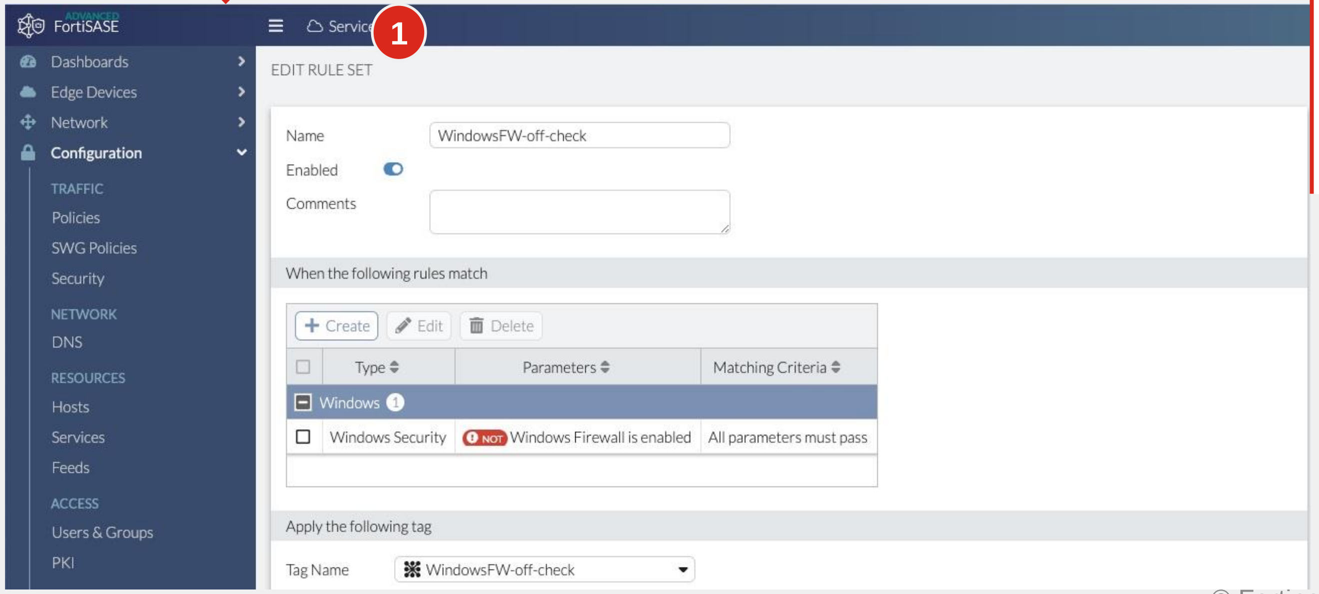
Name	Profile Group	Source	User	Destination	Action	Hit Count	Status
CSA-Thin-Edge-SPA	CSA-SPA-Profile	All Edge Devices		All Private Access Traffic	✓ Accept	2,592	Enabled
ftnt-tk-spa-deny		WindowsFW-off-check	sighber-corp ftnt-tk	All Private Access Traffic	⊘ Deny	0	Enabled
ftnt-tk-spa	Default	WindowsFW-on-c k Win10-OS-check	sighber-corp ftnt-tk	All Private Access Traffic	✓ Accept	8	Enabled
CJ_SPA_Policy	CJ_SPA_Profile_Group	Win10-OS-check WindowsFW-on-c k	CJ_Group	All Private Access Traffic	✓ Accept	3	Enabled
BDE-CAN_VPN_PA_Pol1 Permit DNS	BDE-CAN_PA_PG		BDE-CAN BDE-CAN_FSELAB_RG01	BDE-CAN_PA_DC01	✓ Accept	6,179	Enabled
BDE-CAN_VPN_PA_Pol2 Permit Any	BDE-CAN_PA_PG	BDE-CAN_Domai SELAB	BDE-CAN BDE-CAN_FSELAB_RG01	BDE-CAN_PA_Net_AG	✓ Accept	18,485	Enabled
BDE-CAN_VPN_PA_Pol3 Deny Any			BDE-CAN BDE-CAN_FSELAB_RG01	BDE-CAN_PA_Net_AG	⊘ Deny	106,222	Enabled



Operating System: Windows

Rule Type: AntiVirus

AntiVirus



EDIT RULE SET

Name: WindowsFW-off-check

Enabled

Comments

When the following rules match

Type	Parameters	Matching Criteria
Windows 1		
Windows Security	NOT Windows Firewall is enabled	All parameters must pass

Apply the following tag

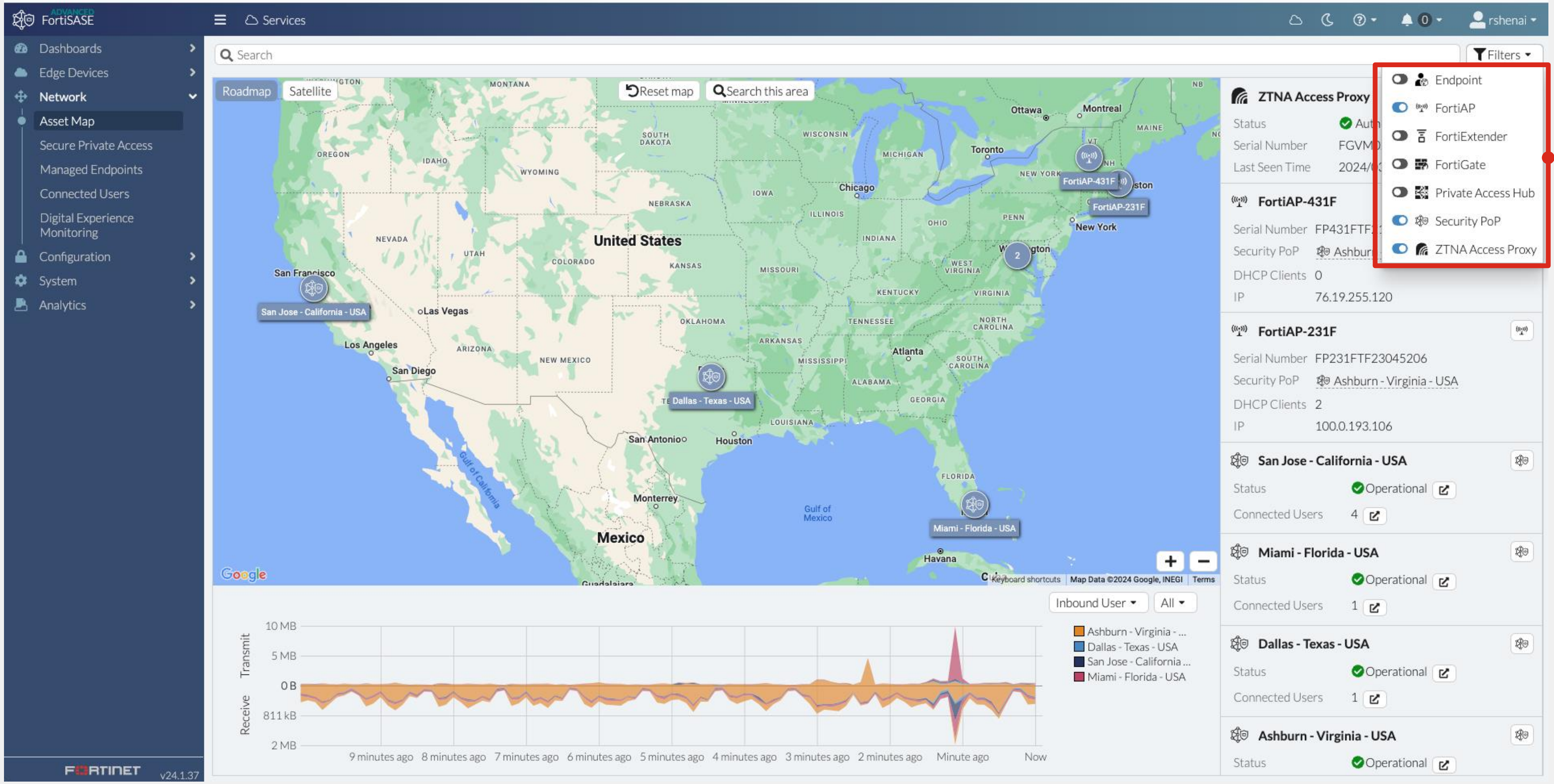
Tag Name: WindowsFW-off-check

1 SPA policies defined with ZTNA tags

2 ZTNA tag rules supported for multiple OS's

FortiSASE Secure Private Access

Bridge to securely connect remote users to their private applications



- ○ Endpoint
- ● FortiAP
- ○ FortiExtender
- ○ FortiGate
- ○ Private Access Hub
- ● Security PoP
- ● ZTNA Access Proxy

ZTNA Access Proxy

Status ✓ Aut
Serial Number FGVM
Last Seen Time 2024/

FortiAP-431F

Serial Number FP431FTF
Security PoP Ashbur
DHCP Clients 0
IP 76.19.255.120

FortiAP-231F

Serial Number FP231FTF23045206
Security PoP Ashburn - Virginia - USA
DHCP Clients 2
IP 100.0.193.106

San Jose - California - USA

Status ✓ Operational
Connected Users 4

Miami - Florida - USA

Status ✓ Operational
Connected Users 1

Dallas - Texas - USA

Status ✓ Operational
Connected Users 1

Ashburn - Virginia - USA

Status ✓ Operational

Filter by Edges

Secure SaaS Access

For Visibility and Control

Secure Access to Cloud apps and files

Cloud App Access Control

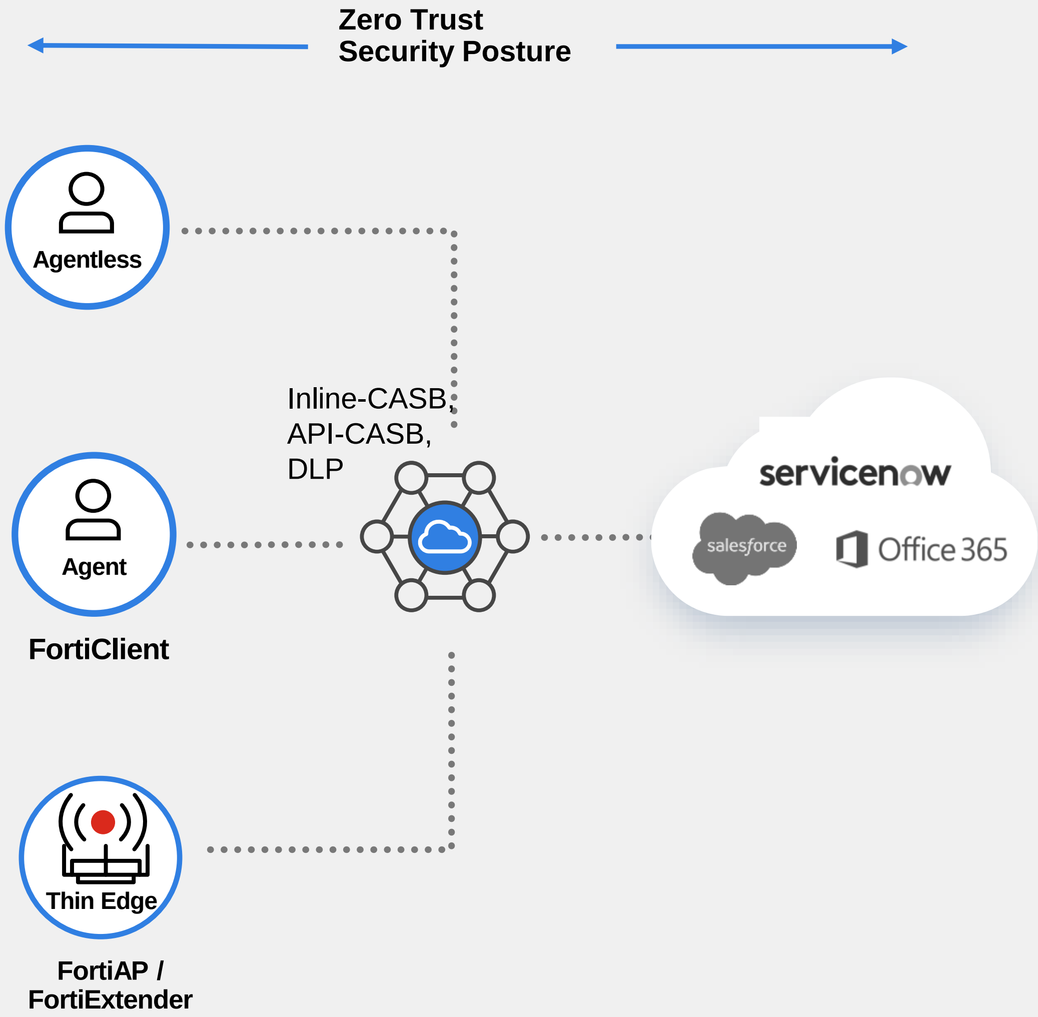
Safe Cloud Application access and blocking of malicious apps with in-line CASB feature, including Zero Trust posture checks

Deep control & view of apps content

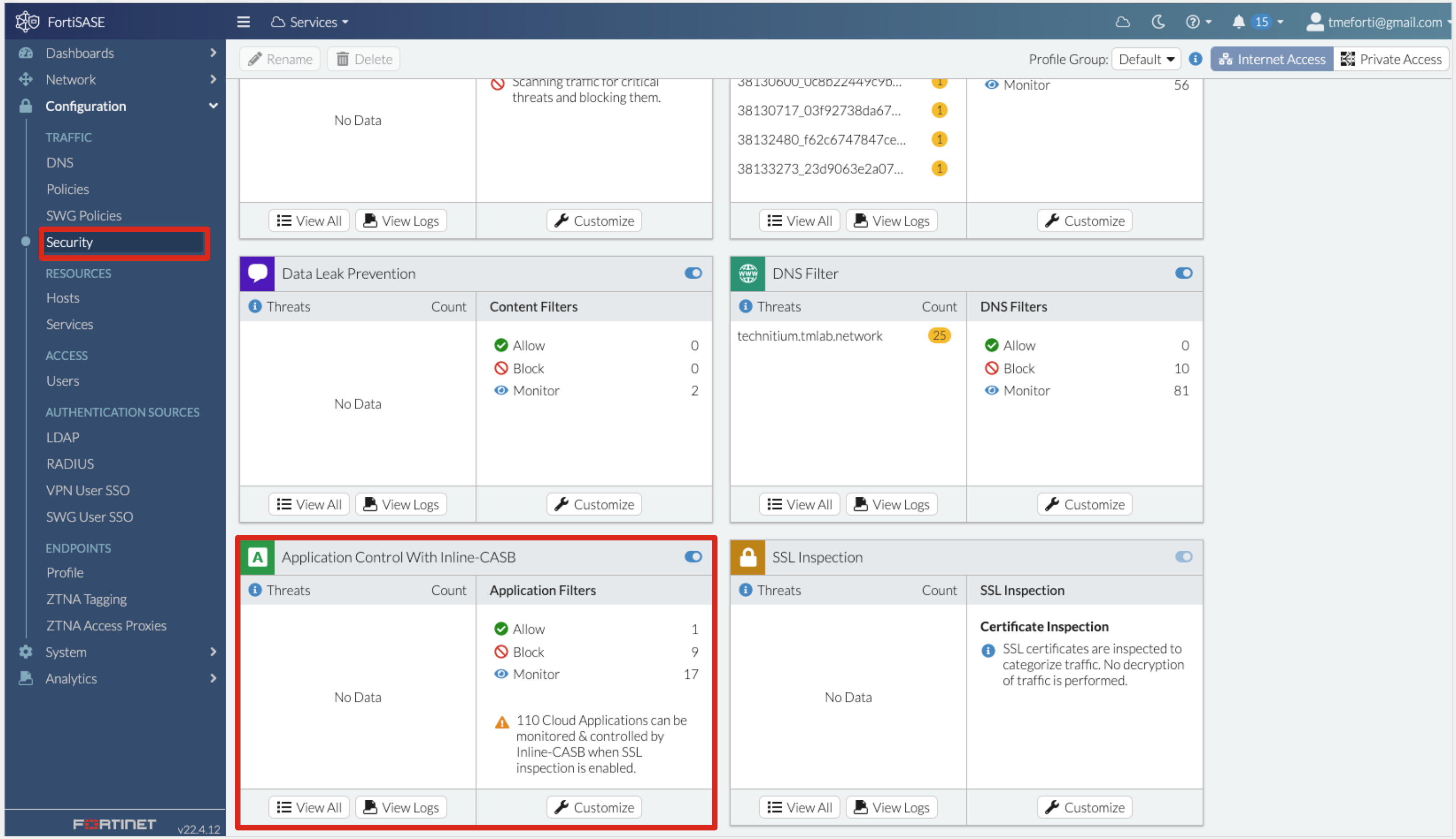
Control over app content and files with API-based CASB for enhanced security and threat detection

Unified agent for anywhere detection

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



Inline CASB capabilities



FortiSASE ☰ Services ▾ 🔔 15 ▾ tmeforti@gmail.com ▾

Dashboards ›
Network ›
Configuration ⌄
TRAFFIC
DNS
Policies
SWG Policies
Security
RESOURCES
Hosts
Services
ACCESS
Users
AUTHENTICATION SOURCES
LDAP
RADIUS
VPN User SSO
SWG User SSO
ENDPOINTS
Profile
ZTNA Tagging
ZTNA Access Proxies
System ›
Analytics ›
FORTINET v22.4.12

Rename Delete Profile Group: Default ▾ Internet Access Private Access

No Data

Scanning traffic for critical threats and blocking them.

38130600_0c8b22449c9b... 1
38130717_03f92738da67... 1
38132480_f62c6747847ce... 1
38133273_23d9063e2a07... 1

Monitor 56

View All View Logs Customize View All View Logs Customize

Data Leak Prevention

Threats	Count	Content Filters	
No Data		Allow	0
		Block	0
		Monitor	2

View All View Logs Customize

DNS Filter

Threats	Count	DNS Filters	
technitium.tmlab.network	25	Allow	0
		Block	10
		Monitor	81

View All View Logs Customize

Application Control With Inline-CASB

Threats	Count	Application Filters	
No Data		Allow	1
		Block	9
		Monitor	17

⚠ 110 Cloud Applications can be monitored & controlled by Inline-CASB when SSL inspection is enabled.

View All View Logs Customize

SSL Inspection

Threats	Count	SSL Inspection
No Data		**Certificate Inspection** SSL certificates are inspected to categorize traffic. No decryption of traffic is performed.

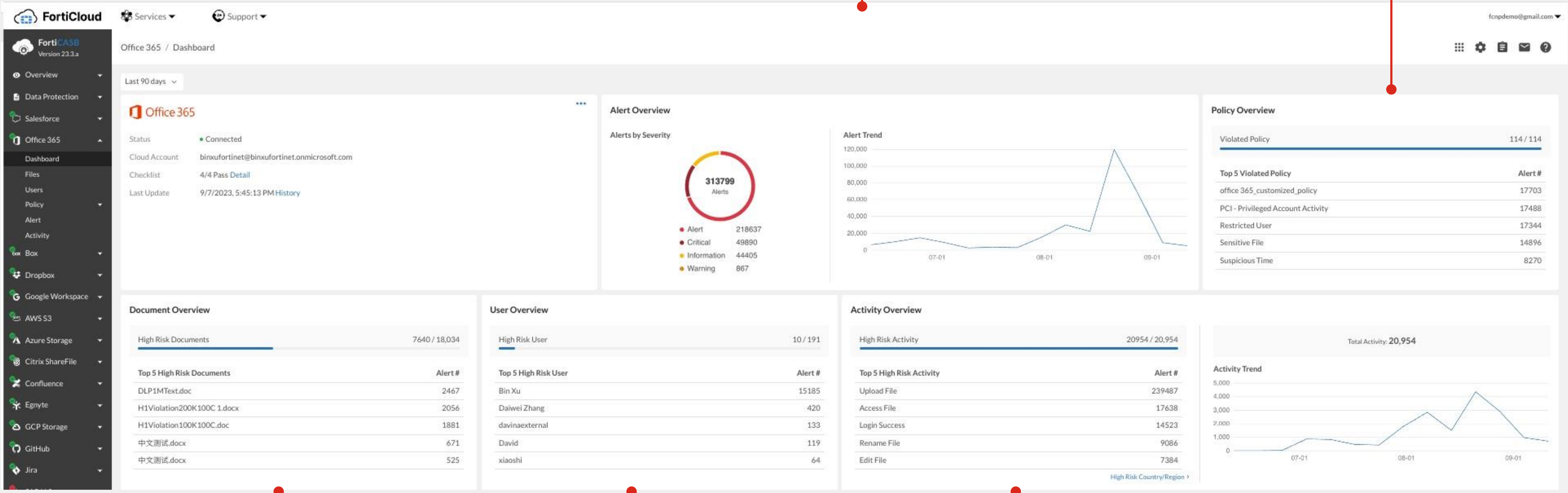
View All View Logs Customize

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

Example: O365 Summary Over Past 90 Days

Alerts & Trends

Policy Violations



Office 365 / Dashboard

Last 90 days

Office 365

Status	● Connected
Cloud Account	binxufortinet@binxufortinet.onmicrosoft.com
Checklist	4/4 Pass Detail
Last Update	9/7/2023, 5:45:13 PM History

Alert Overview

Alerts by Severity

● Alert	218637
● Critical	49890
● Information	44405
● Warning	867

Alert Trend

Policy Overview

Violated Policy 114 / 114

Top 5 Violated Policy	Alert #
office 365_customized_policy	17703
PCI - Privileged Account Activity	17488
Restricted User	17344
Sensitive File	14896
Suspicious Time	8270

Document Overview

High Risk Documents 7640 / 18,034

Top 5 High Risk Documents	Alert #
DLP1MText.doc	2467
H1Violation200K100C 1.docx	2056
H1Violation100K100C.doc	1881
中文测试.docx	671
中文测试.docx	525

User Overview

High Risk User 10 / 191

Top 5 High Risk User	Alert #
Bin Xu	15185
Daiwei Zhang	420
davinaexternal	133
David	119
xiaoshi	64

Activity Overview

High Risk Activity 20954 / 20,954

Top 5 High Risk Activity	Alert #
Upload File	239487
Access File	17638
Login Success	14523
Rename File	9086
Edit File	7384

High Risk Country/Region ›

Total Activity: 20,954

Activity Trend

Documents profiled as per Risk

Users profiled as per Risk

Activities profiled as per Risk

Comprehensive Data Security

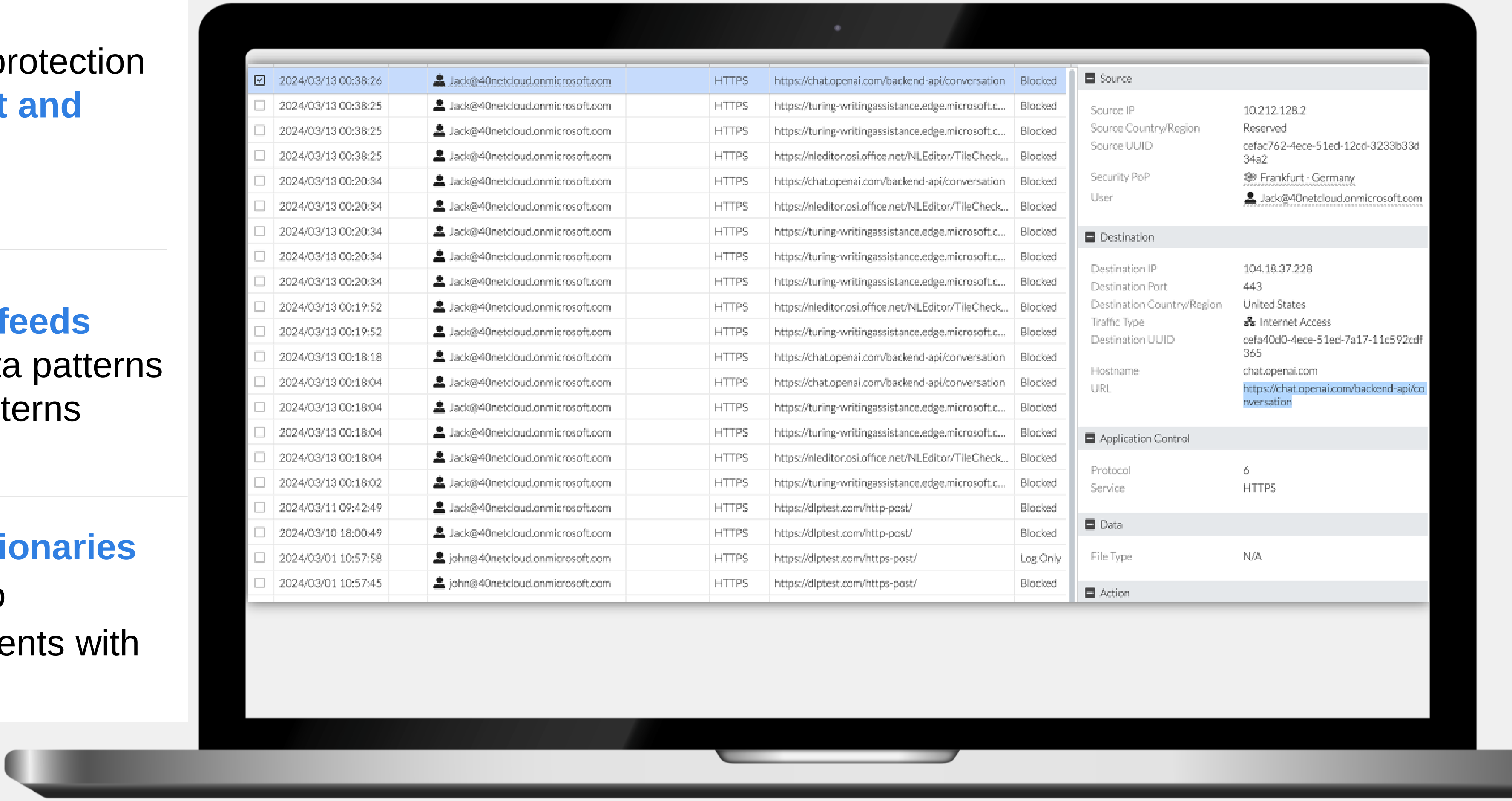
Built-in Data Leakage Protection (DLP)

Data Protection with FortiSASE

Identification, monitoring and protection of organization's data—**At rest and in motion**

FortiGuard AI-powered DLP feeds
Supports 500+ pre-defined data patterns updated frequently for new patterns

Predefined sensors and dictionaries
Support for granular policies to meet data protection requirements with tailored reporting



☑	2024/03/13 00:38:26	Jack@40netcloud.onmicrosoft.com	HTTPS	https://chat.openai.com/backend-api/conversation	Blocked
□	2024/03/13 00:38:25	Jack@40netcloud.onmicrosoft.com	HTTPS	https://turing-writingassistance.edge.microsoft.c...	Blocked
□	2024/03/13 00:38:25	Jack@40netcloud.onmicrosoft.com	HTTPS	https://turing-writingassistance.edge.microsoft.c...	Blocked
□	2024/03/13 00:38:25	Jack@40netcloud.onmicrosoft.com	HTTPS	https://nleditor.osi.office.net/NLEditor/TileCheck...	Blocked
□	2024/03/13 00:20:34	Jack@40netcloud.onmicrosoft.com	HTTPS	https://chat.openai.com/backend-api/conversation	Blocked
□	2024/03/13 00:20:34	Jack@40netcloud.onmicrosoft.com	HTTPS	https://nleditor.osi.office.net/NLEditor/TileCheck...	Blocked
□	2024/03/13 00:20:34	Jack@40netcloud.onmicrosoft.com	HTTPS	https://turing-writingassistance.edge.microsoft.c...	Blocked
□	2024/03/13 00:20:34	Jack@40netcloud.onmicrosoft.com	HTTPS	https://turing-writingassistance.edge.microsoft.c...	Blocked
□	2024/03/13 00:20:34	Jack@40netcloud.onmicrosoft.com	HTTPS	https://turing-writingassistance.edge.microsoft.c...	Blocked
□	2024/03/13 00:19:52	Jack@40netcloud.onmicrosoft.com	HTTPS	https://nleditor.osi.office.net/NLEditor/TileCheck...	Blocked
□	2024/03/13 00:19:52	Jack@40netcloud.onmicrosoft.com	HTTPS	https://turing-writingassistance.edge.microsoft.c...	Blocked
□	2024/03/13 00:18:18	Jack@40netcloud.onmicrosoft.com	HTTPS	https://chat.openai.com/backend-api/conversation	Blocked
□	2024/03/13 00:18:04	Jack@40netcloud.onmicrosoft.com	HTTPS	https://chat.openai.com/backend-api/conversation	Blocked
□	2024/03/13 00:18:04	Jack@40netcloud.onmicrosoft.com	HTTPS	https://turing-writingassistance.edge.microsoft.c...	Blocked
□	2024/03/13 00:18:04	Jack@40netcloud.onmicrosoft.com	HTTPS	https://turing-writingassistance.edge.microsoft.c...	Blocked
□	2024/03/13 00:18:04	Jack@40netcloud.onmicrosoft.com	HTTPS	https://nleditor.osi.office.net/NLEditor/TileCheck...	Blocked
□	2024/03/13 00:18:02	Jack@40netcloud.onmicrosoft.com	HTTPS	https://turing-writingassistance.edge.microsoft.c...	Blocked
□	2024/03/11 09:42:49	Jack@40netcloud.onmicrosoft.com	HTTPS	https://dlptest.com/http-post/	Blocked
□	2024/03/10 18:00:49	Jack@40netcloud.onmicrosoft.com	HTTPS	https://dlptest.com/http-post/	Blocked
□	2024/03/01 10:57:58	john@40netcloud.onmicrosoft.com	HTTPS	https://dlptest.com/https-post/	Log Only
□	2024/03/01 10:57:45	john@40netcloud.onmicrosoft.com	HTTPS	https://dlptest.com/https-post/	Blocked

Source

Source IP	10.212.128.2
Source Country/Region	Reserved
Source UUID	cefac762-4ece-51ed-12cd-3233b33d34a2
Security PoP	Frankfurt - Germany
User	Jack@40netcloud.onmicrosoft.com

Destination

Destination IP	104.18.37.228
Destination Port	443
Destination Country/Region	United States
Traffic Type	Internet Access
Destination UUID	cefa40d0-4ece-51ed-7a17-11c592cdf365
Hostname	chat.openai.com
URL	https://chat.openai.com/backend-api/conversation

Application Control

Protocol	6
Service	HTTPS

Data

File Type	N/A

Action

Secure Thin Edge Connectivity

Industry's First – Wireless LAN integration with SASE

Secure Thin Edge Access

Cloud delivered AI-powered Security

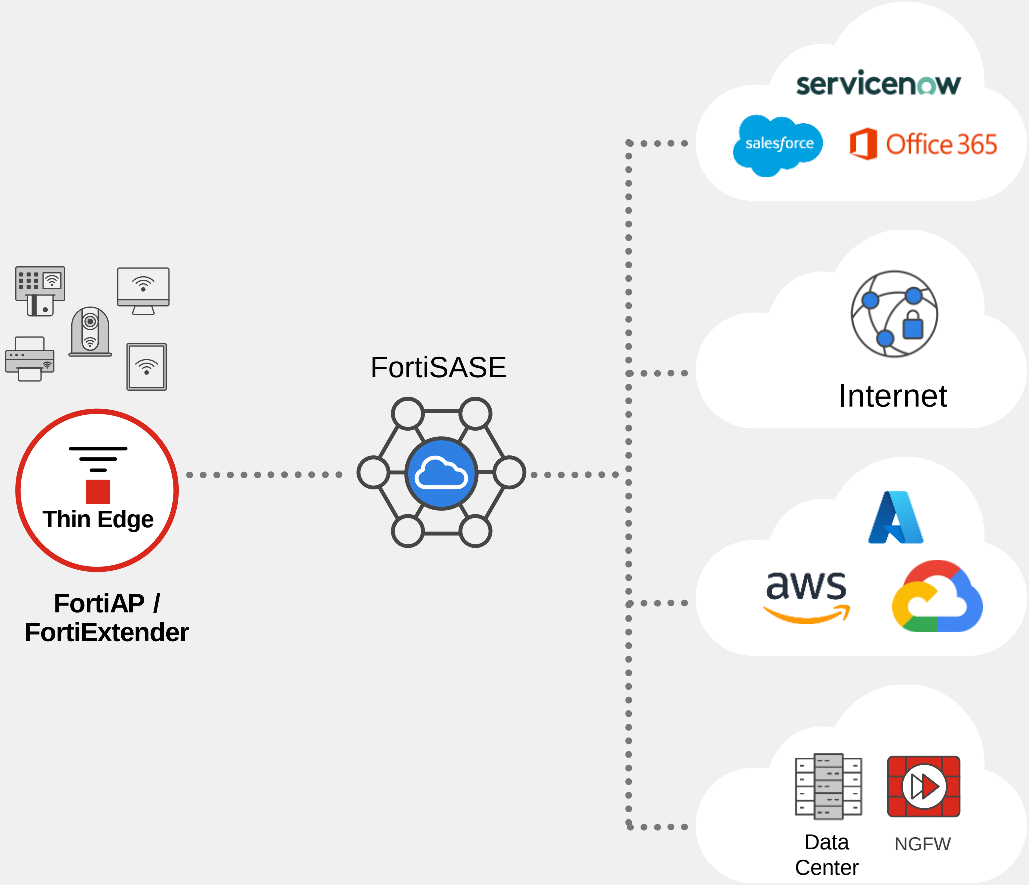
Secure thin edge locations that don't have on-prem firewall to block ransomware and malware

Secure Agentless Access from IoT

Secure access using built-in hardware agent in FortiAP and FortiExtender without any client agents.

Cloud delivered Management

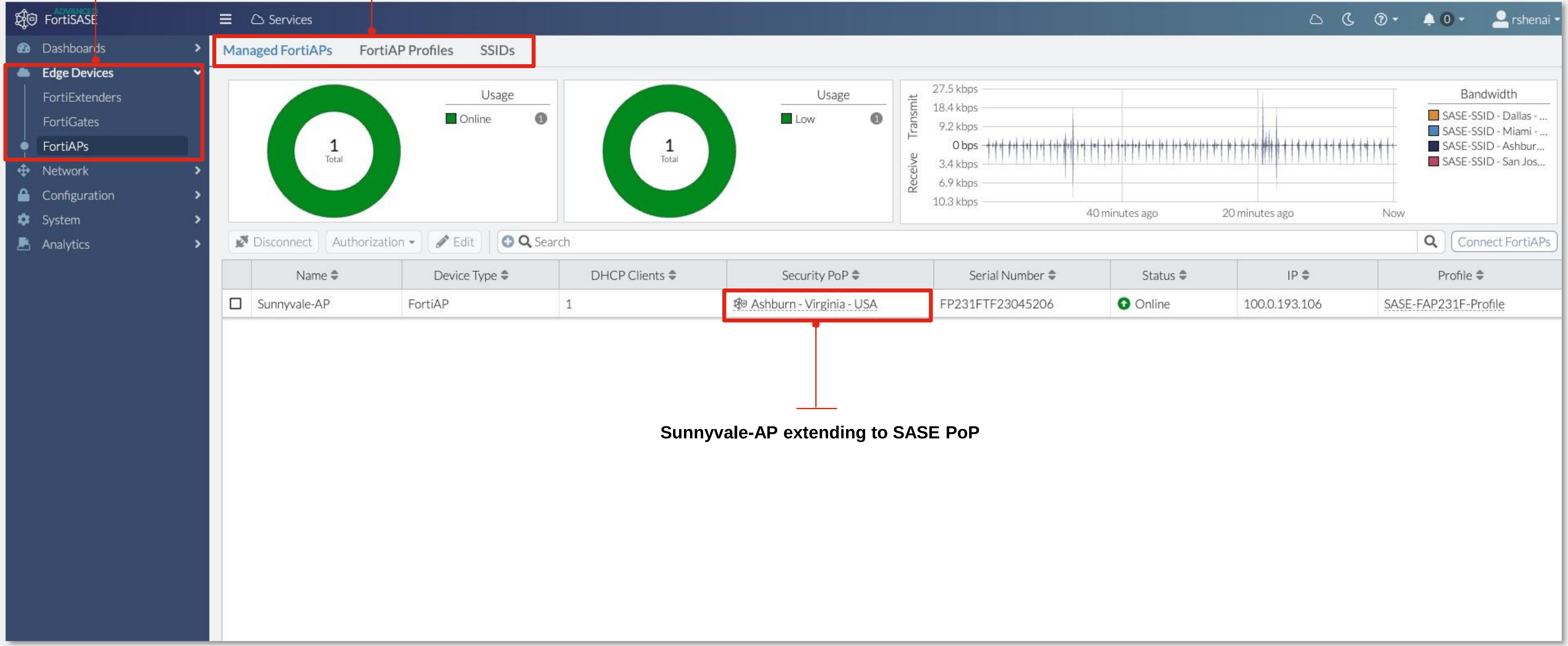
Cloud delivered management of FortiAP and FortiExtender with zero-touch provisioning support



FortiSASE Cloud Delivered Management for Thin Edge

Streamlined Management

Single pane to manage



□	Name	Device Type	DHCP Clients	Security PoP	Serial Number	Status	IP	Profile
□	Sunnyvale-AP	FortiAP	1	Ashburn - Virginia - USA	FP231FTF23045206	Online	100.0.193.106	SASE-FAP231F-Profile

Sunnyvale-AP extending to SASE PoP

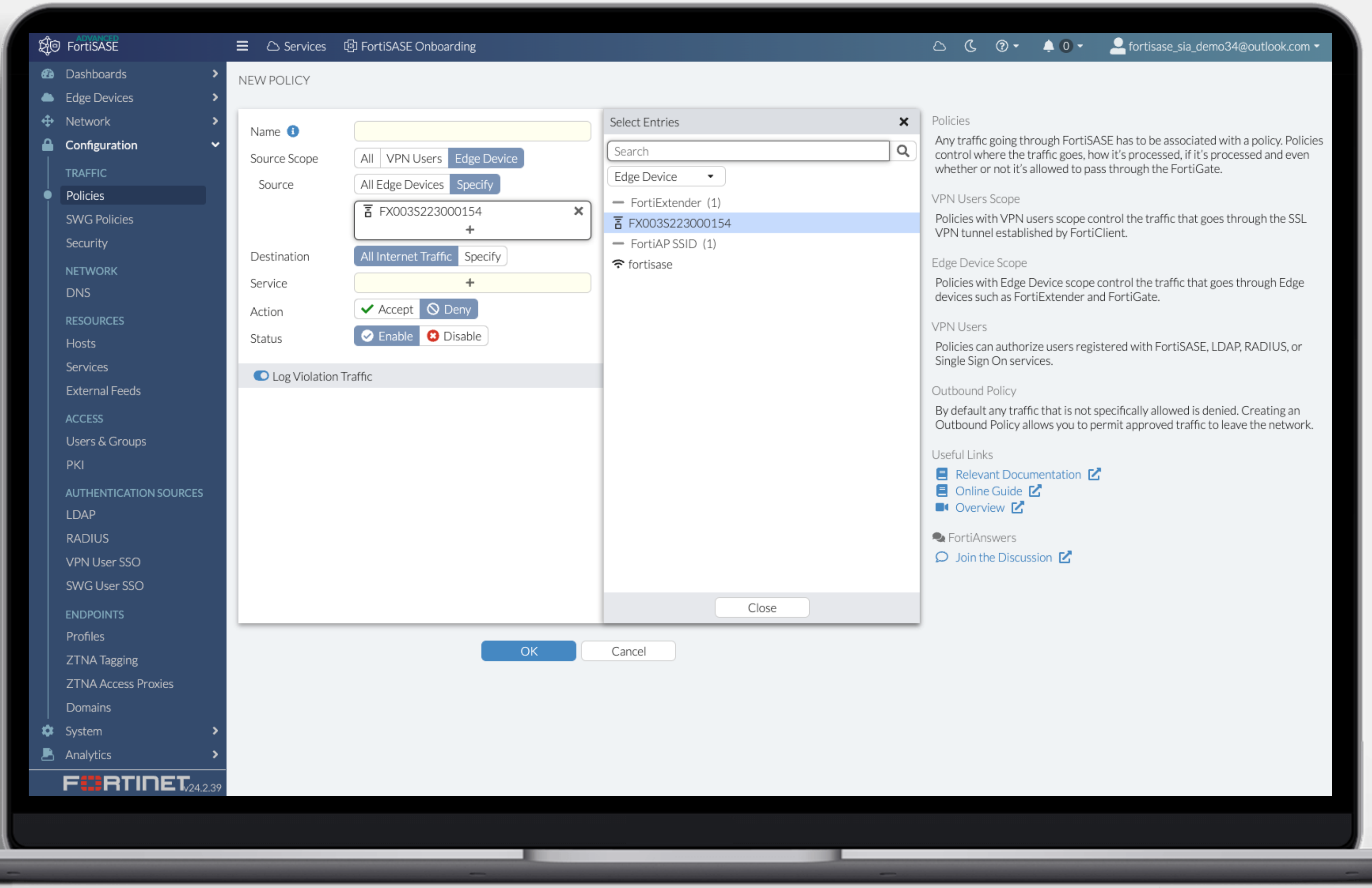
24.2.a

Secure Edge Connectivity - What’s New

Granular Edge Device Security Policies

Granular Edge Policies

- Control Secure Internet Access and Secure Private Access Policies per Edge
- Supports FortiAP SSIDs, FortiExtenders, FortiGate Edge Devices
- Specify Authorized Edge Device as Source



NEW POLICY

Name

Source Scope: All | VPN Users | Edge Device

Source: All Edge Devices | Specify

FX003S223000154

Destination: All Internet Traffic | Specify

Service

Action: Accept | Deny

Status: Enable | Disable

Log Violation Traffic

Select Entries

Search

Edge Device

- FortiExtender (1)
- FX003S223000154
- FortiAP SSID (1)
- fortisase

Close

OK Cancel

Policies

Any traffic going through FortiSASE has to be associated with a policy. Policies control where the traffic goes, how it’s processed, if it’s processed and even whether or not it’s allowed to pass through the FortiGate.

VPN Users Scope

Policies with VPN users scope control the traffic that goes through the SSL VPN tunnel established by FortiClient.

Edge Device Scope

Policies with Edge Device scope control the traffic that goes through Edge devices such as FortiExtender and FortiGate.

VPN Users

Policies can authorize users registered with FortiSASE, LDAP, RADIUS, or Single Sign On services.

Outbound Policy

By default any traffic that is not specifically allowed is denied. Creating an Outbound Policy allows you to permit approved traffic to leave the network.

Useful Links

Relevant Documentation
Online Guide
Overview

FortiAnswers

Join the Discussion

Free FortiSASE with FortiAP 431F in 2024

Experience FortiSASE cloud delivered security and management with FortiAP 431F

Purchase new FortiAP 431F

Register FortiAP in FortiCloud account

Use promo code “**2024-SASE-AP**” during FortiSASE provisioning

Use zero touch provisioning tool to connect FortiAP to FortiSASE

Connect FortiAP to FortiSASE for free cloud security through Dec 31, 2024

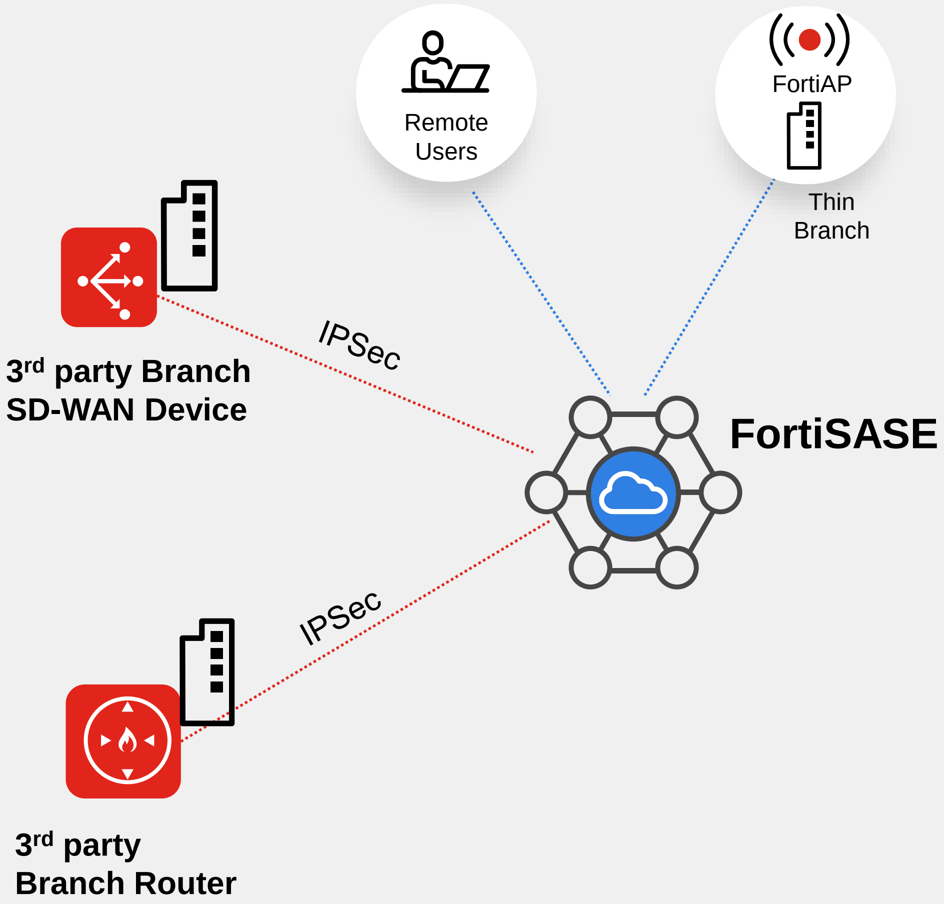
Full Details on the Web

Secure Edge Connectivity – What's New

SD-WAN On Ramp for Branch

IPSec Connectivity to FortiSASE from Branch

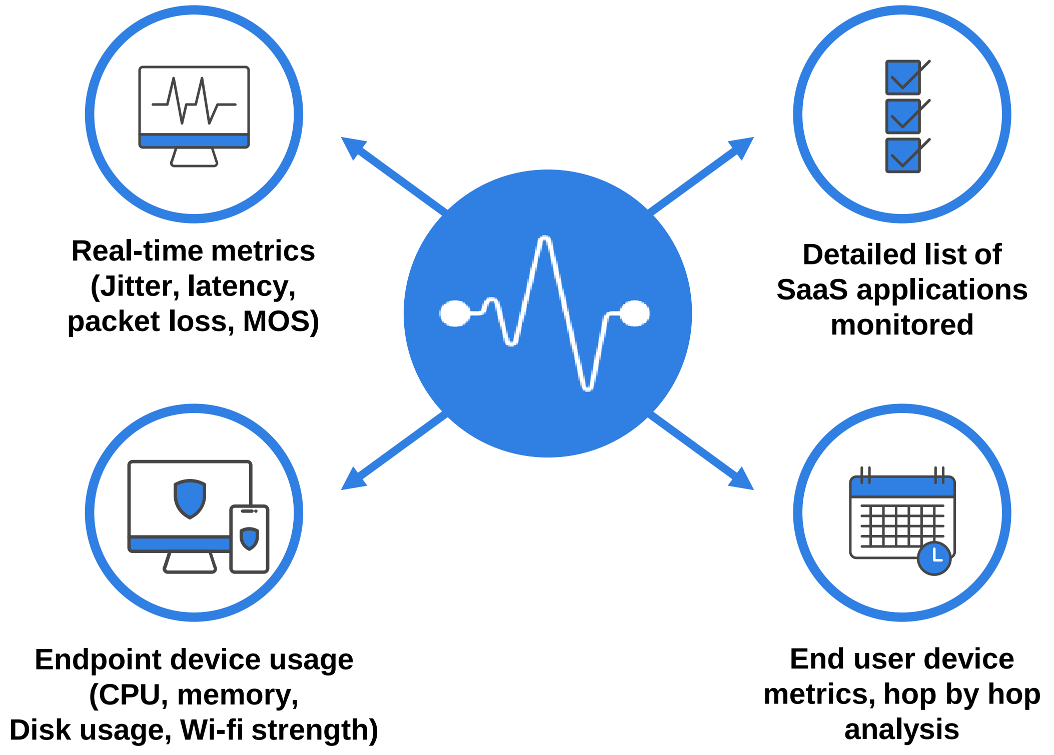
- Extends FortiSASE to all branch edge locations
- Supports IPSec from any validated branch edge device to connect to FortiSASE
- Supports IPSec connection to 2 FortiSASE locations per branch for redundancy
- Requires Add-on for **SD-WAN On-Ramp** per FortiSASE Location (Advanced or Comprehensive)



Advanced features

End-to-End Digital Experience Monitoring

Comprehensive visibility | Metrics and alerts correlation | Proactive response

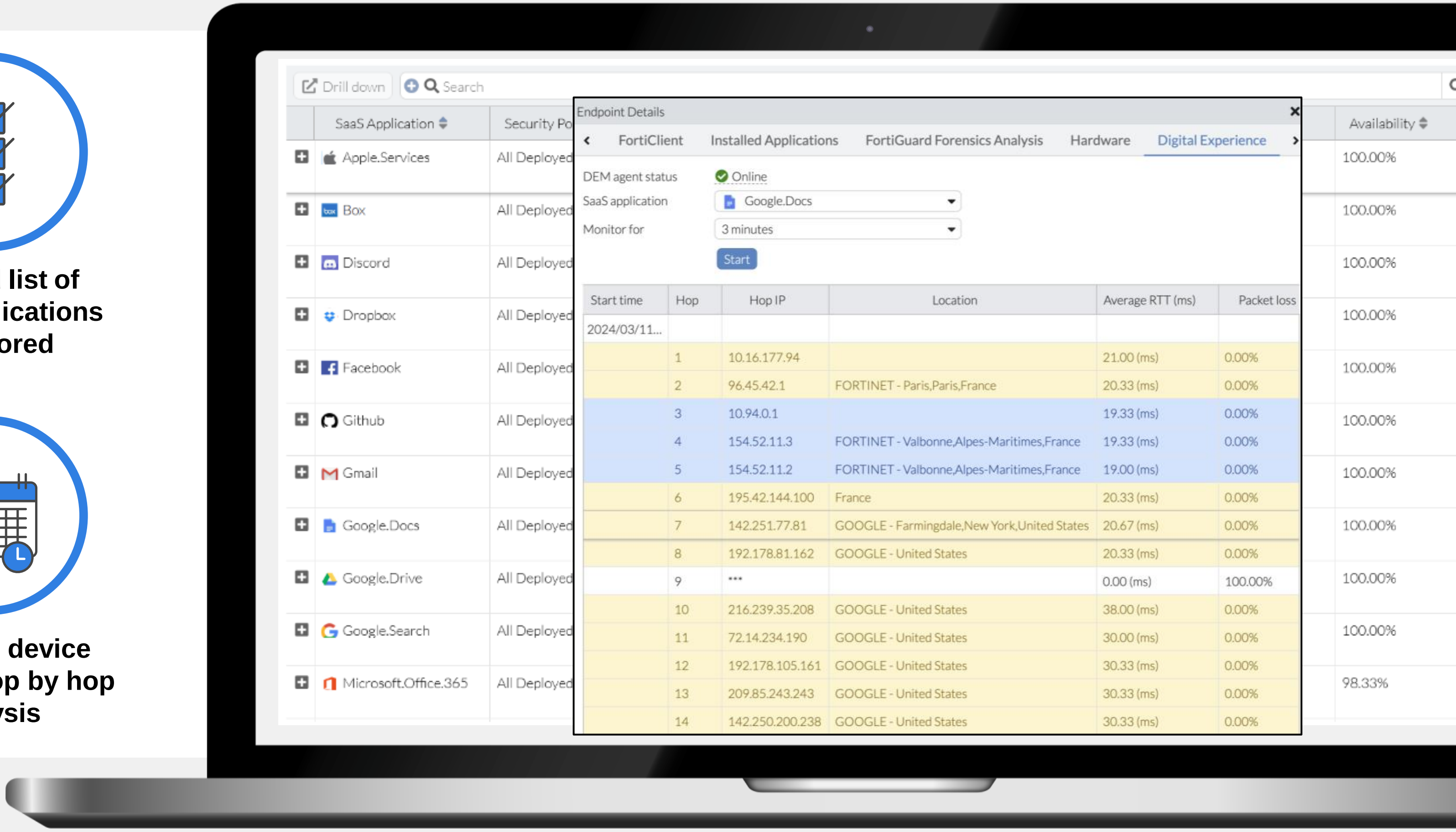


Real-time metrics (Jitter, latency, packet loss, MOS)

Detailed list of SaaS applications monitored

Endpoint device usage (CPU, memory, Disk usage, Wi-fi strength)

End user device metrics, hop by hop analysis



SaaS Application	Security Po	Availability
Apple.Services	All Deployed	100.00%
Box	All Deployed	100.00%
Discord	All Deployed	100.00%
Dropbox	All Deployed	100.00%
Facebook	All Deployed	100.00%
Github	All Deployed	100.00%
Gmail	All Deployed	100.00%
Google.Docs	All Deployed	100.00%
Google.Drive	All Deployed	100.00%
Google.Search	All Deployed	100.00%
Microsoft.Office.365	All Deployed	98.33%

Endpoint Details

DEM agent status: Online

SaaS application: Google.Docs

Monitor for: 3 minutes

Start time	Hop	Hop IP	Location	Average RTT (ms)	Packet loss
2024/03/11...					
	1	10.16.177.94		21.00 (ms)	0.00%
	2	96.45.42.1	FORTINET - Paris,Paris,France	20.33 (ms)	0.00%
	3	10.94.0.1		19.33 (ms)	0.00%
	4	154.52.11.3	FORTINET - Valbonne,Alpes-Maritimes,France	19.33 (ms)	0.00%
	5	154.52.11.2	FORTINET - Valbonne,Alpes-Maritimes,France	19.00 (ms)	0.00%
	6	195.42.144.100	France	20.33 (ms)	0.00%
	7	142.251.77.81	GOOGLE - Farmingdale,New York,United States	20.67 (ms)	0.00%
	8	192.178.81.162	GOOGLE - United States	20.33 (ms)	0.00%
	9	***		0.00 (ms)	100.00%
	10	216.239.35.208	GOOGLE - United States	38.00 (ms)	0.00%
	11	72.14.234.190	GOOGLE - United States	30.00 (ms)	0.00%
	12	192.178.105.161	GOOGLE - United States	30.33 (ms)	0.00%
	13	209.85.243.243	GOOGLE - United States	30.33 (ms)	0.00%
	14	142.250.200.238	GOOGLE - United States	30.33 (ms)	0.00%

SOC As a Service integration with FortiSASE

Seamless integration

Say No to False Positives!

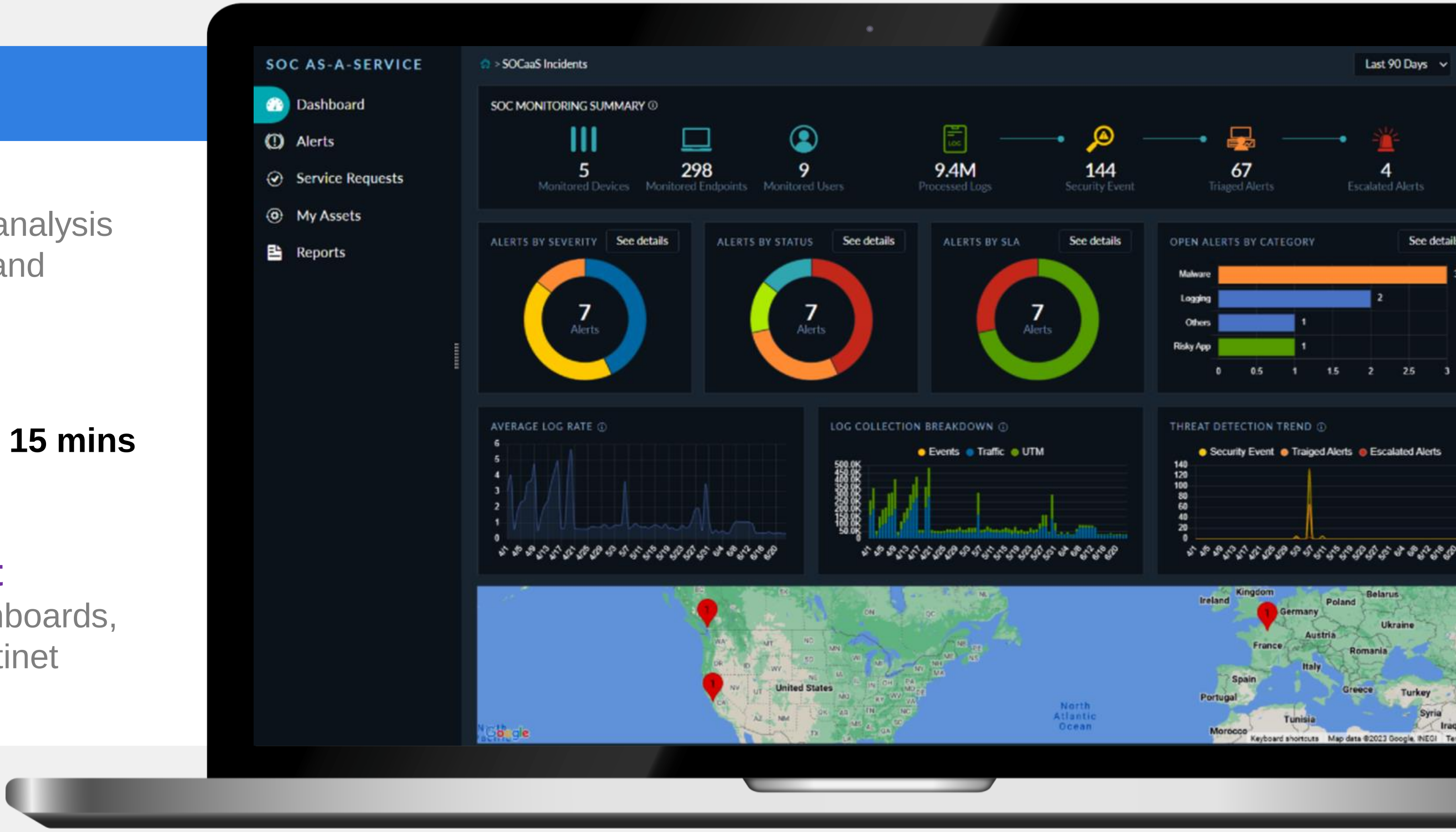
24x7 Human based Monitoring and analysis with weekly summary reports, alerts and notifications

Respond: Act Fast

Fortinet security experts notify **within 15 mins** – IOCs, remediation, why and what

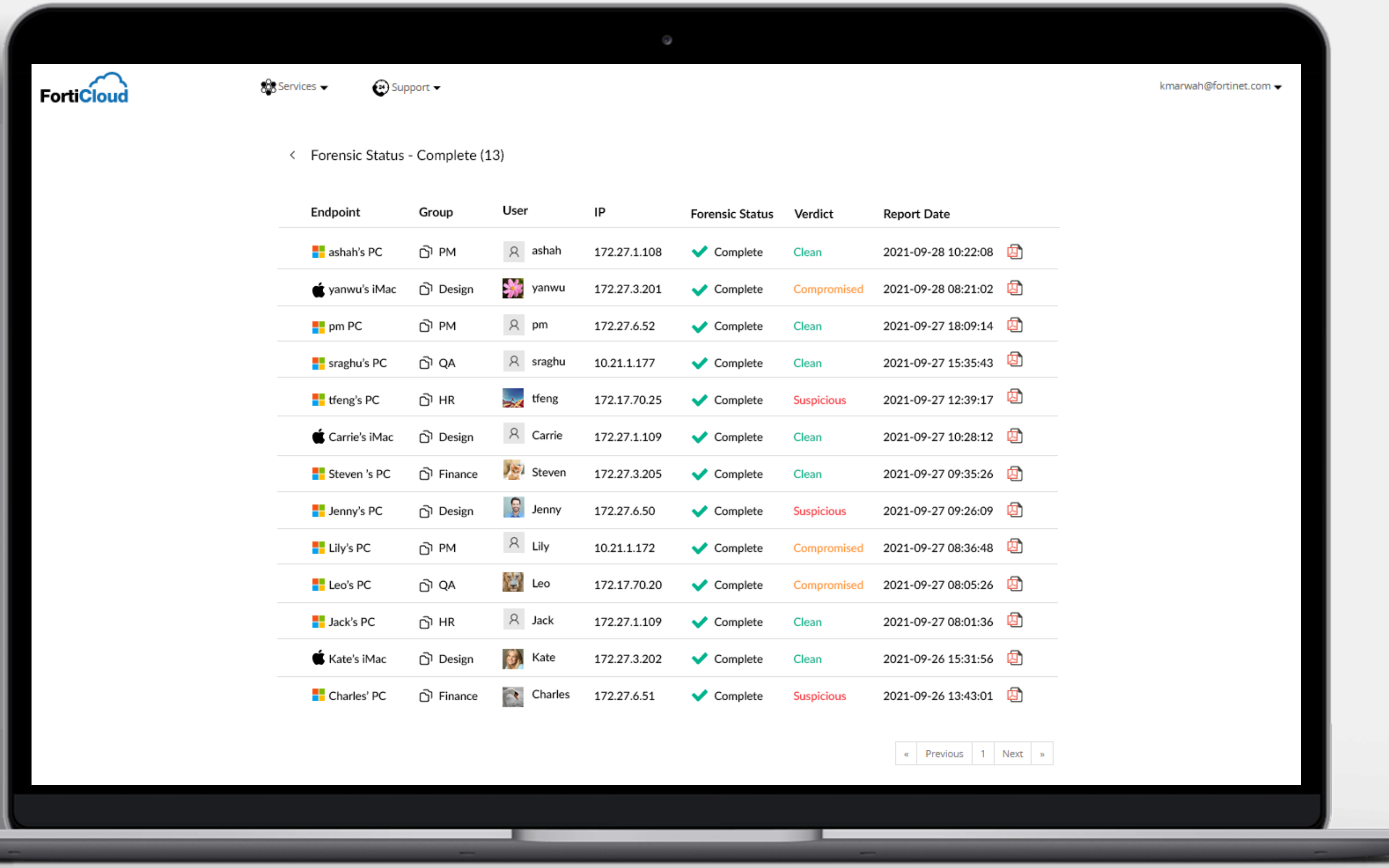
Improve: Maximize Investment

Cloud-based portal with intuitive dashboards, on-demand reports and quarterly Fortinet **expert meetings**



Security – FortiGuard Forensics

- Leverage FortiGuard Forensics service to investigate potentially compromised endpoints
- Submit Endpoints for analysis directly from the FortiSASE portal
- FortiGuard Forensics Team will analyze and provide verdict & details report on findings



Forensic Status - Complete (13)

Endpoint	Group	User	IP	Forensic Status	Verdict	Report Date
ashah's PC	PM	ashah	172.27.1.108	✓ Complete	Clean	2021-09-28 10:22:08
yanwu's iMac	Design	yanwu	172.27.3.201	✓ Complete	Compromised	2021-09-28 08:21:02
pm PC	PM	pm	172.27.6.52	✓ Complete	Clean	2021-09-27 18:09:14
sraghu's PC	QA	sraghu	10.21.1.177	✓ Complete	Clean	2021-09-27 15:35:43
tfeng's PC	HR	tfeng	172.17.70.25	✓ Complete	Suspicious	2021-09-27 12:39:17
Carrie's iMac	Design	Carrie	172.27.1.109	✓ Complete	Clean	2021-09-27 10:28:12
Steven 's PC	Finance	Steven	172.27.3.205	✓ Complete	Clean	2021-09-27 09:35:26
Jenny's PC	Design	Jenny	172.27.6.50	✓ Complete	Suspicious	2021-09-27 09:26:09
Lily's PC	PM	Lily	10.21.1.172	✓ Complete	Compromised	2021-09-27 08:36:48
Leo's PC	QA	Leo	172.17.70.20	✓ Complete	Compromised	2021-09-27 08:05:26
Jack's PC	HR	Jack	172.27.1.109	✓ Complete	Clean	2021-09-27 08:01:36
Kate's iMac	Design	Kate	172.27.3.202	✓ Complete	Clean	2021-09-26 15:31:56
Charles' PC	Finance	Charles	172.27.6.51	✓ Complete	Suspicious	2021-09-26 13:43:01

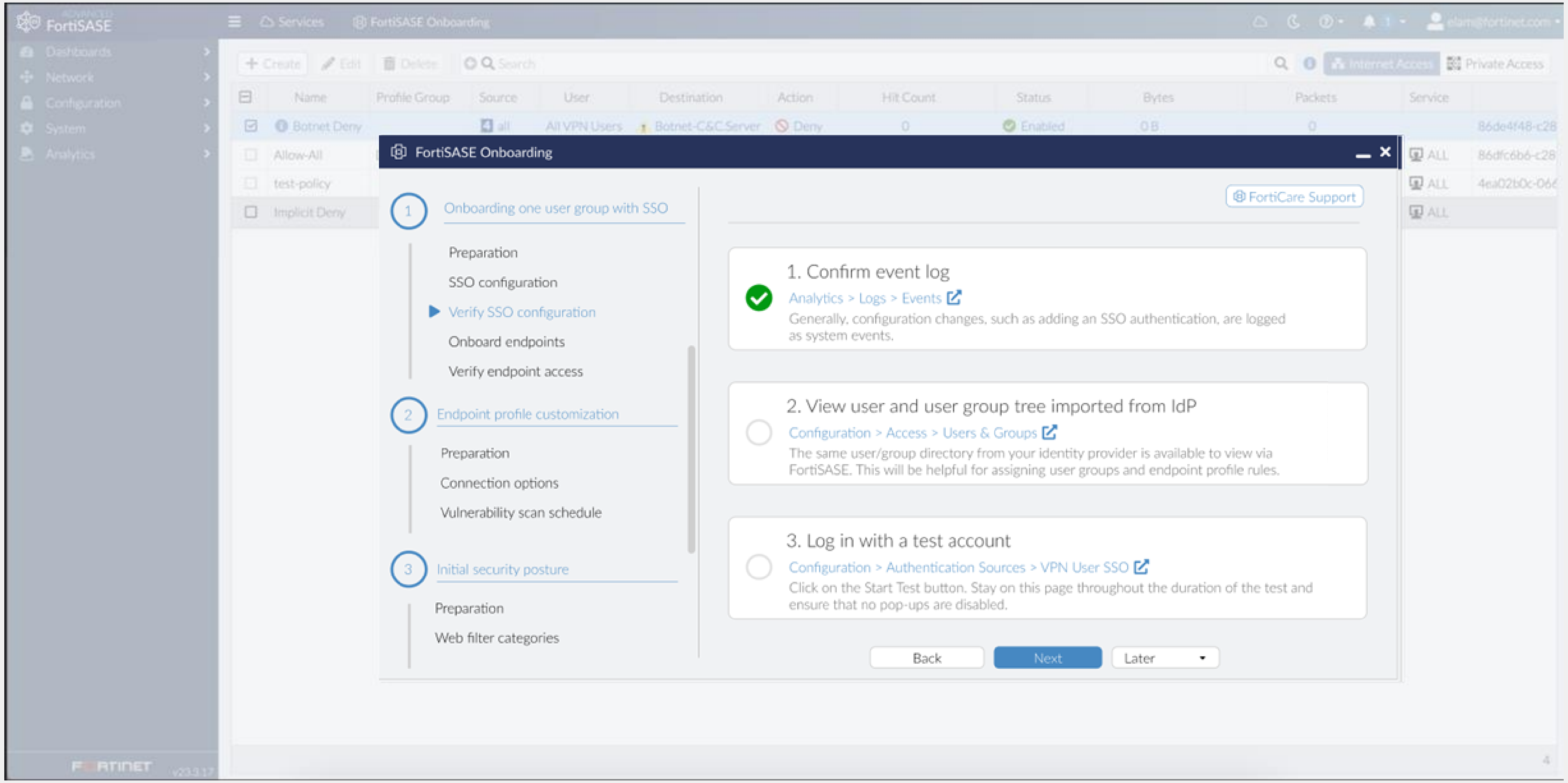
Assisted Onboarding

Define

- Understand your environment and any unique requirements
- Capture relevant configuration for the Deploy phase

Deploy

- Embedded guides will assist you through the deployment of common scenarios:
- *Enable Authentication*
- *On-board Users & Devices*
- *Link with SD-WAN network*



1 Onboarding one user group with SSO

- Preparation
- SSO configuration
- ▶ Verify SSO configuration
- Onboard endpoints
- Verify endpoint access

2 Endpoint profile customization

- Preparation
- Connection options
- Vulnerability scan schedule

3 Initial security posture

- Preparation
- Web filter categories

✓ 1. Confirm event log

Analytics > Logs > Events

Generally, configuration changes, such as adding an SSO authentication, are logged as system events.

○ 2. View user and user group tree imported from IdP

Configuration > Access > Users & Groups

The same user/group directory from your identity provider is available to view via FortiSASE. This will be helpful for assigning user groups and endpoint profile rules.

○ 3. Log in with a test account

Configuration > Authentication Sources > VPN User SSO

Click on the Start Test button. Stay on this page throughout the duration of the test and ensure that no pop-ups are disabled.

Pricing

Simple SASE Licensing

Includes all SASE features under single user-based SKU

FortiSASE Pricing

"Fortinet provides excellent value and it’s BOMs are the simplest of any vendor in the SASE market"

- 2024 Gartner Single Vendor SASE MQ

FortiSASE Standard Bundle

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

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

CASB & DLP : In-line CASB, API CASB and DLP Service

Endpoint Security : EPP, Sandboxing, Vulnerability Management

Cloud Logging

Cloud Managed

24 x 7 Support

Supports 3 devices per user

Summary of FortiSASE Bundles and What's New

Capability	Standard	Advanced	Comprehensive
SWG	●	●	●
FWaaS	●	●	●
FortiClient & EPP	●	●	●
ZTNA	●	●	●
CASB (Inline and API)	●	●	●
Data Loss Prevention (DLP)	●	●	●
Sandbox	●	●	●
Digital Experience Monitoring		●	●
SOCaaS Integration		●	●
Endpoint Forensics		●	●
Dedicated IPs	*Add-on*	●	●
Assisted On-boarding		●	●
POPs	*Fortinet Cloud Locations*	*Fortinet Cloud Locations*	*All Locations*
Consumption	*Yearly or FortiFlex*	*Yearly or FortiFlex*	*Yearly or FortiFlex*

New – Customers can have up-to 20 PoPs

Both Fortinet & Public Cloud Locations can be used

Now available for use within FortiFlex

See FortiSASE Ordering Guide Link for more details

Why Fortinet Unified SASE?

1

FortiOS Powered Convergence

FortiOS

2

AI / ML Driven FortiGuard Security

AI-Security

3

Simplicity

Unified agent
Single console
SOCaaS / DEM

4

Flexible Security

Flexible deployment
Flexible locations
Agentless/Agent

Simplifying Operations and Cost Savings

Consistent Security Posture

Better User Experience

FORTINET®