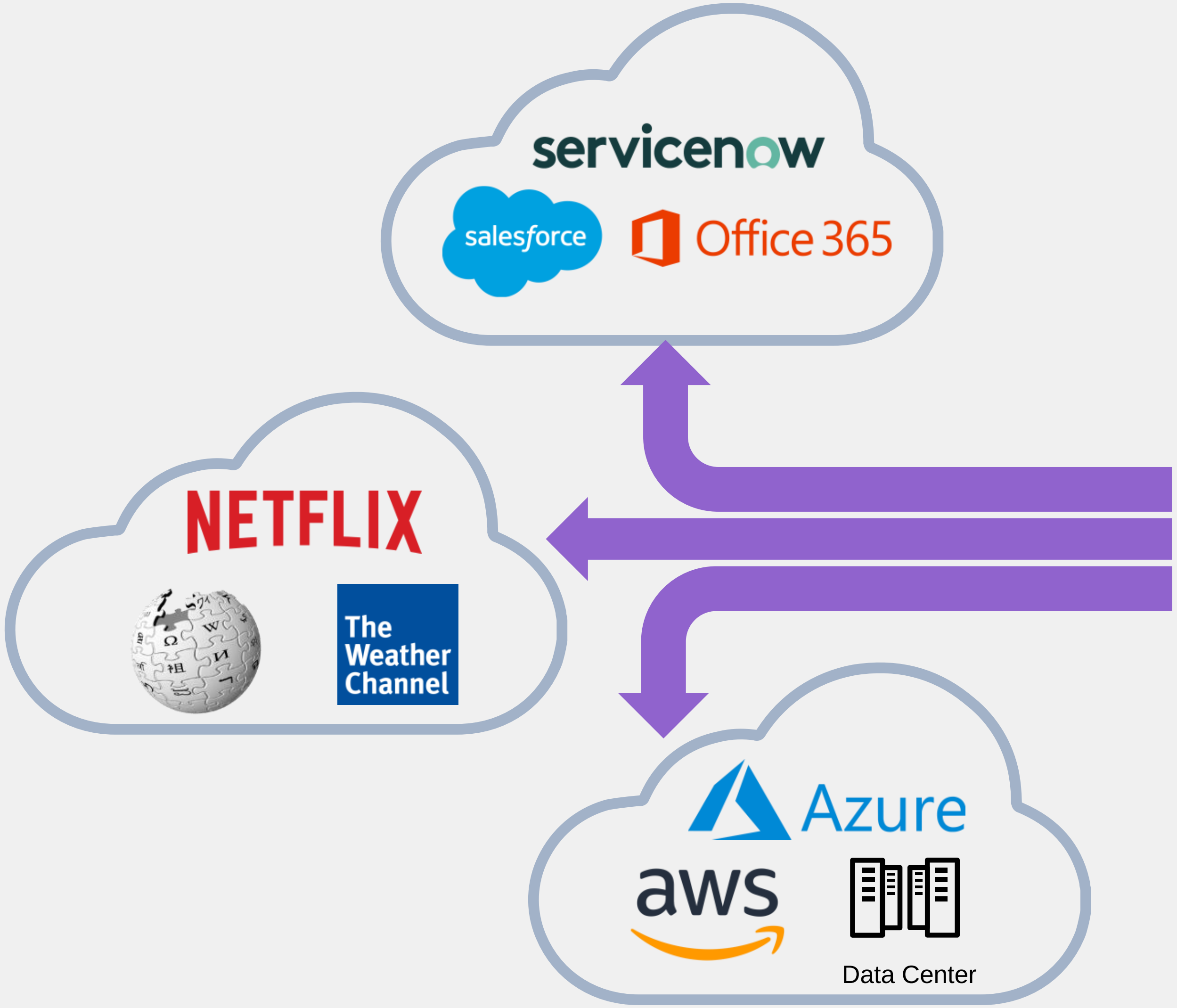
Sicherer Zugang zum Internet, auf Anwendungen im Firmennetzwerk und in die Cloud für ihre hybride Belegschaft: Ein Einblick in FortiSASE

Vitus Zeller, Business Development Manager

Juli 2024

Hybrid Workforce



Market Trends

Hybrid Workforce

84%

SOURCE 1:
2023 Forbes Remote Work Trends

Distributed Applications

125+

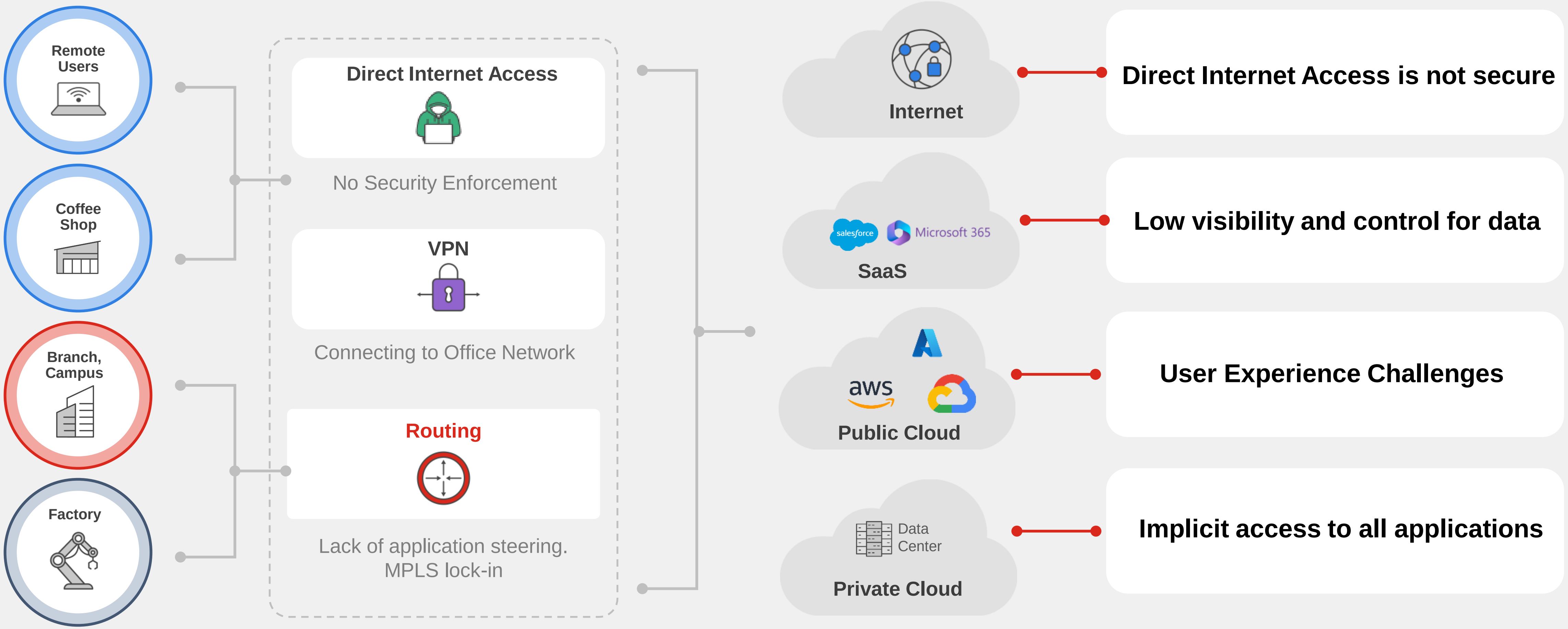
SOURCE 2:
2022 Gartner: Market Guide for SaaS Management Platforms

Active Vendor Consolidation

75%

SOURCE 3:
2022 Gartner CISO Survey and infographics

Current Technology Requires Transformation



Direct Internet Access is not secure

Low visibility and control for data

User Experience Challenges

Implicit access to all applications

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

Analyst Recommends SASE for Secure Access

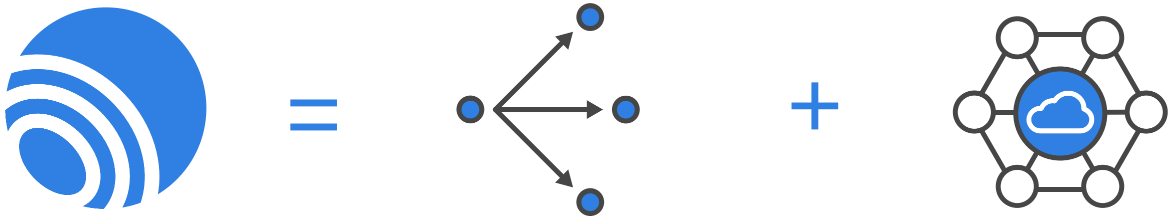
Mindset

Zero Trust Security Posture

Architecture

Secure Access Service Edge (SASE)

Capabilities



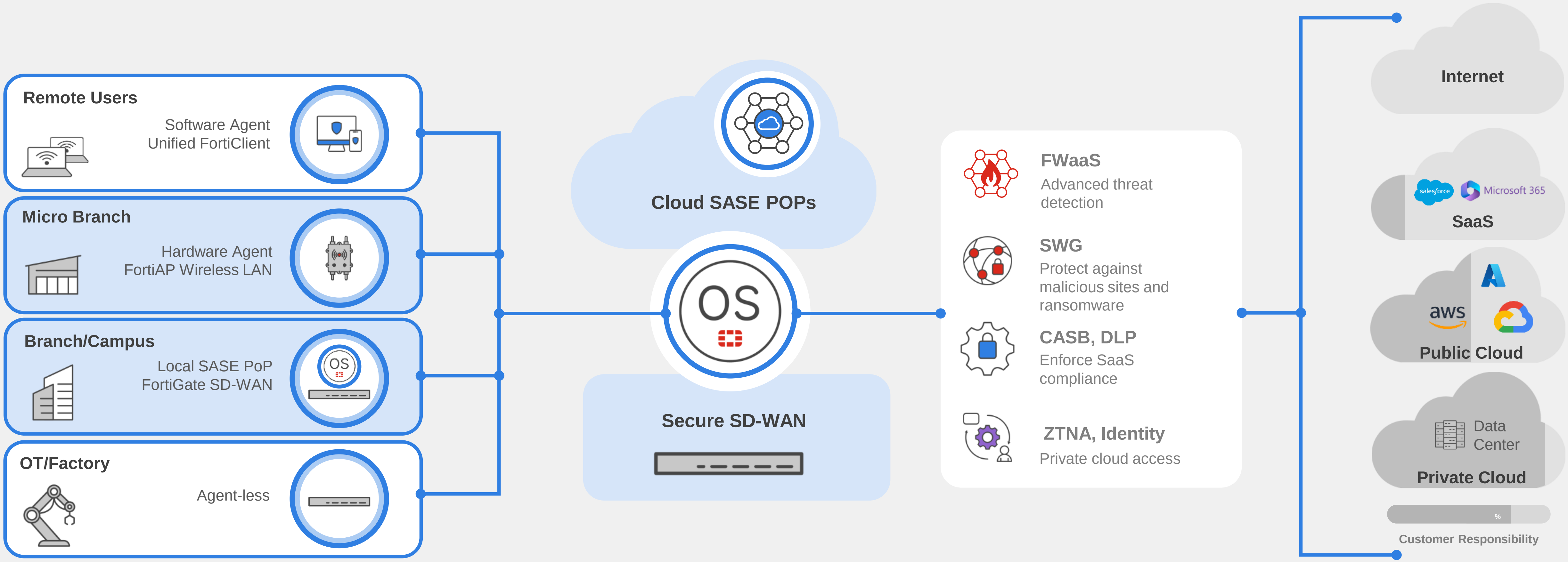
SASE = On-Prem Connectivity + Cloud-Delivered Protection

Outcome

End-to-End Digital Experience with Secure Access

By 2026 – 85% of organizations will adopt SSE offering – Gartner SSE MQ 2024

Hybrid Approach to SASE with Consistent Protection



Remote Users

Software Agent
Unified FortiClient

Micro Branch

Hardware Agent
FortiAP Wireless LAN

Branch/Campus

Local SASE PoP
FortiGate SD-WAN

OT/Factory

Agent-less

Cloud SASE POPs

OS

Secure SD-WAN

FWaaS
Advanced threat detection

SWG
Protect against malicious sites and ransomware

CASB, DLP
Enforce SaaS compliance

ZTNA, Identity
Private cloud access

Internet

salesforce Microsoft 365
SaaS

aws
Public Cloud

Data Center
Private Cloud

%
Customer Responsibility

Unified SASE Use Cases

Secure SD-WAN for Branch and Campus

Transitioning from MPLS to Broadband via SD-WAN reduces cost and enhance application performance.

Clear ROI, Controller-less, Convergence

Secure Internet Access for Remote Users

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

AI-Powered Security, Unified Agent, Unified Management

Upgrade Remote Access for Private Applications

Explicit application access under a zero-trust mindset to ensure secure application access

Real-time Monitoring, Universal Enforcement,

SaaS Control and Data Protection

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

Unified Management, Data Protection

Thin Edge for Secure Access

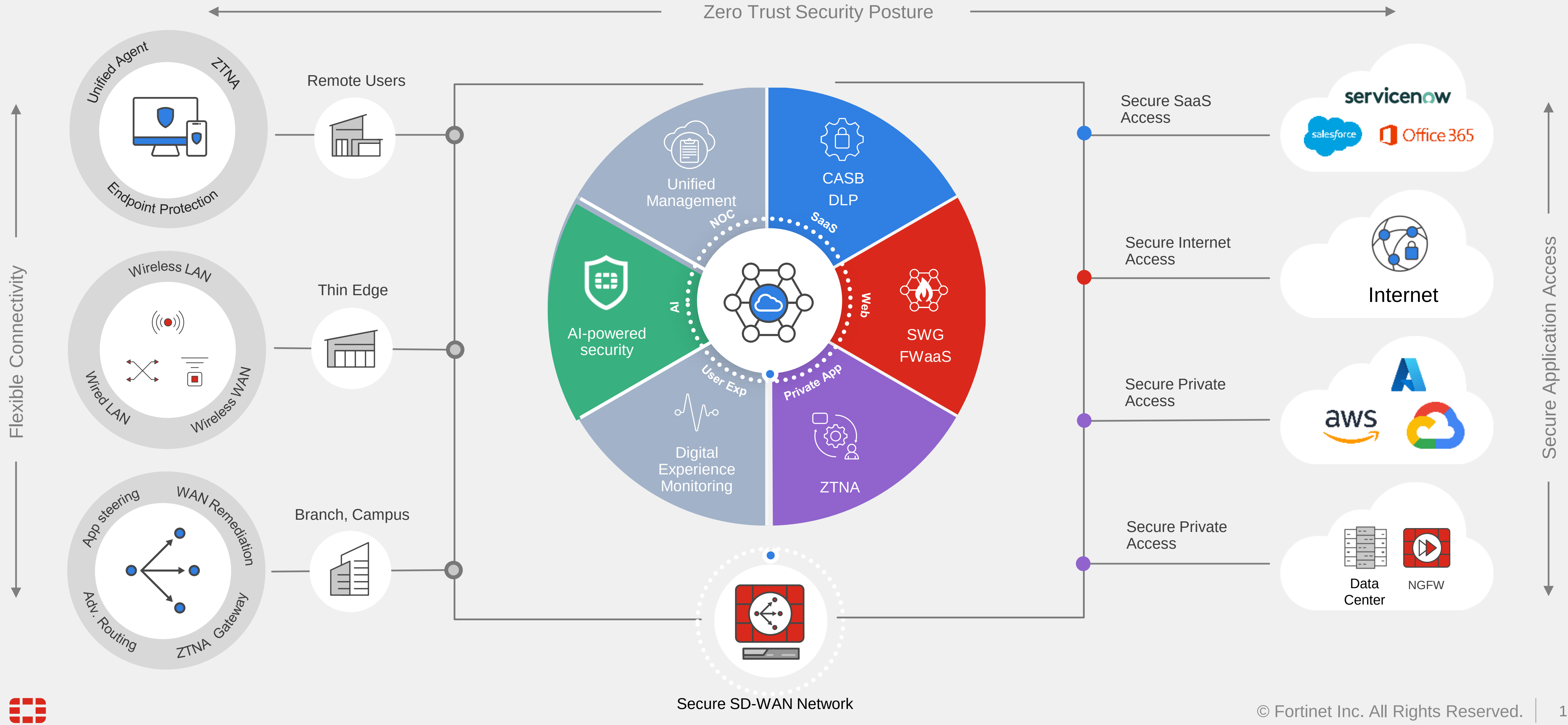
Deploy and manage Access point with SASE and enable secure access for users and unmanaged devices

Industry's Only, Secure Access, Flexible Connectivity

Fortinet SASE Solution

FortiSASE – Cloud Delivered Security Service Edge

Secure access for the hybrid workforce



FortiSASE – One Console for Management and Visibility

FortiSASE Unified Management

Centralized Control

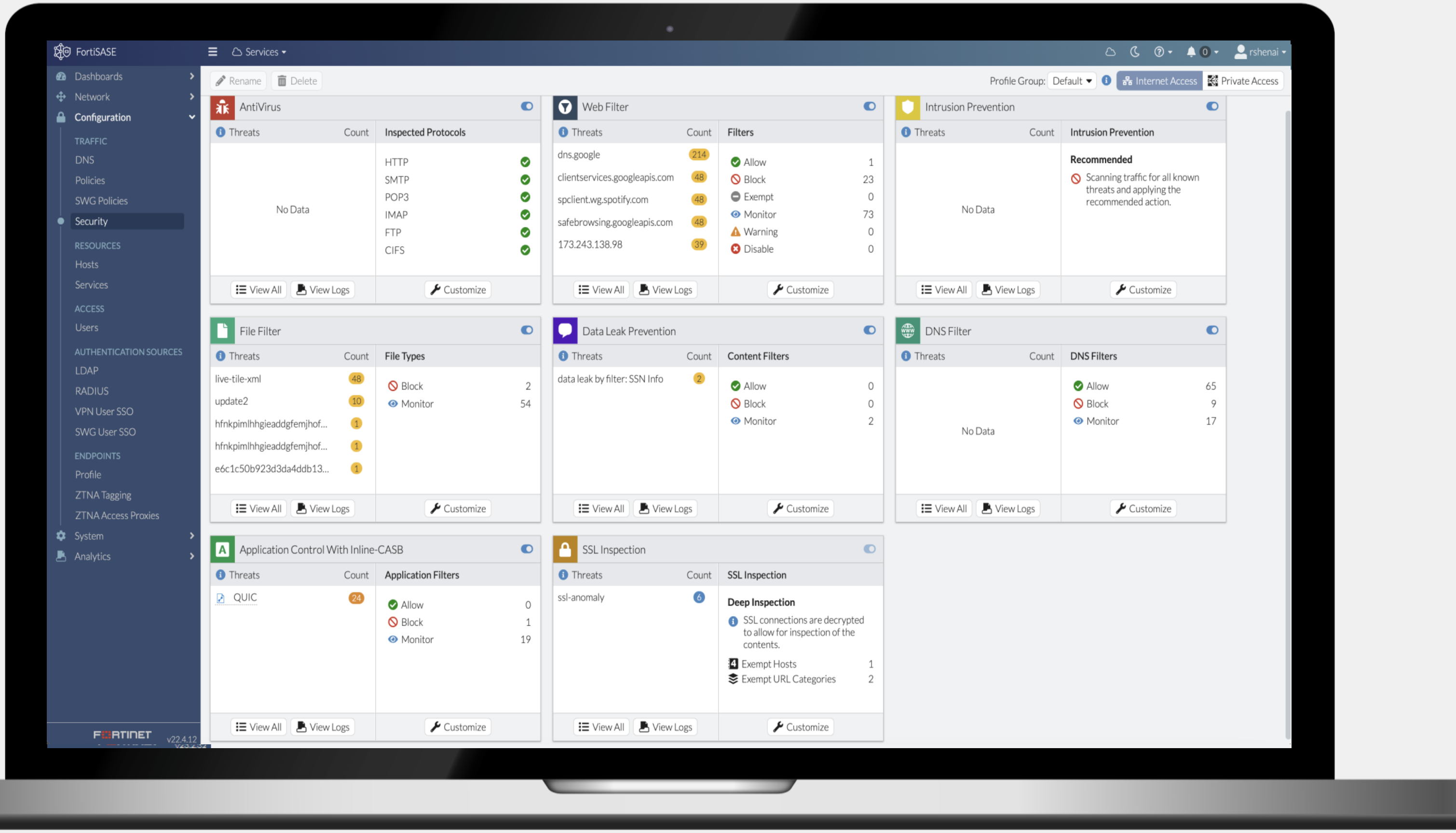
Control and configure all FortiSASE components (SWG, FWaaS, ZTNA, CASB, DLP)

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

Use cases

Secure Internet Access

For Remote Users, Thin Edge and Branch Locations

Safe browsing from anywhere

Malware & Ransomware prevention

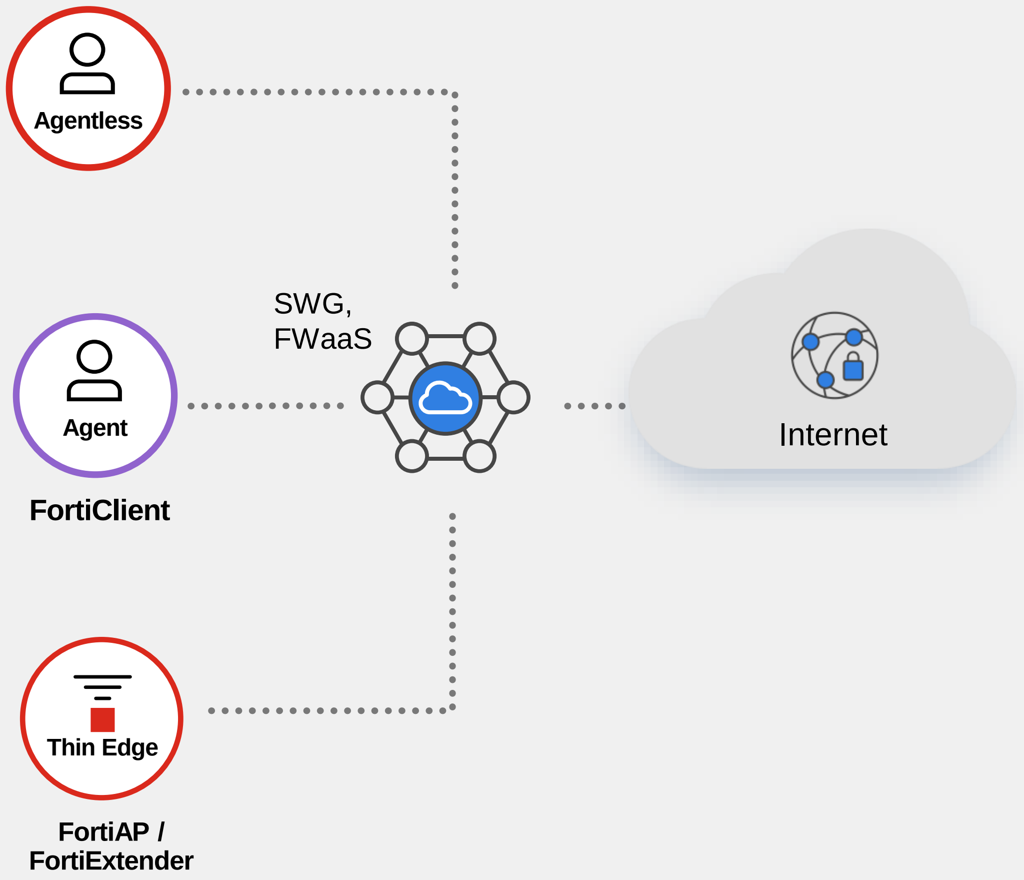
Prevent threats with cloud-based Firewall, IPS, Web Filtering, Anti-virus, DNS and File Filtering, Sandbox

Deep SSL Inspection of end-user activity

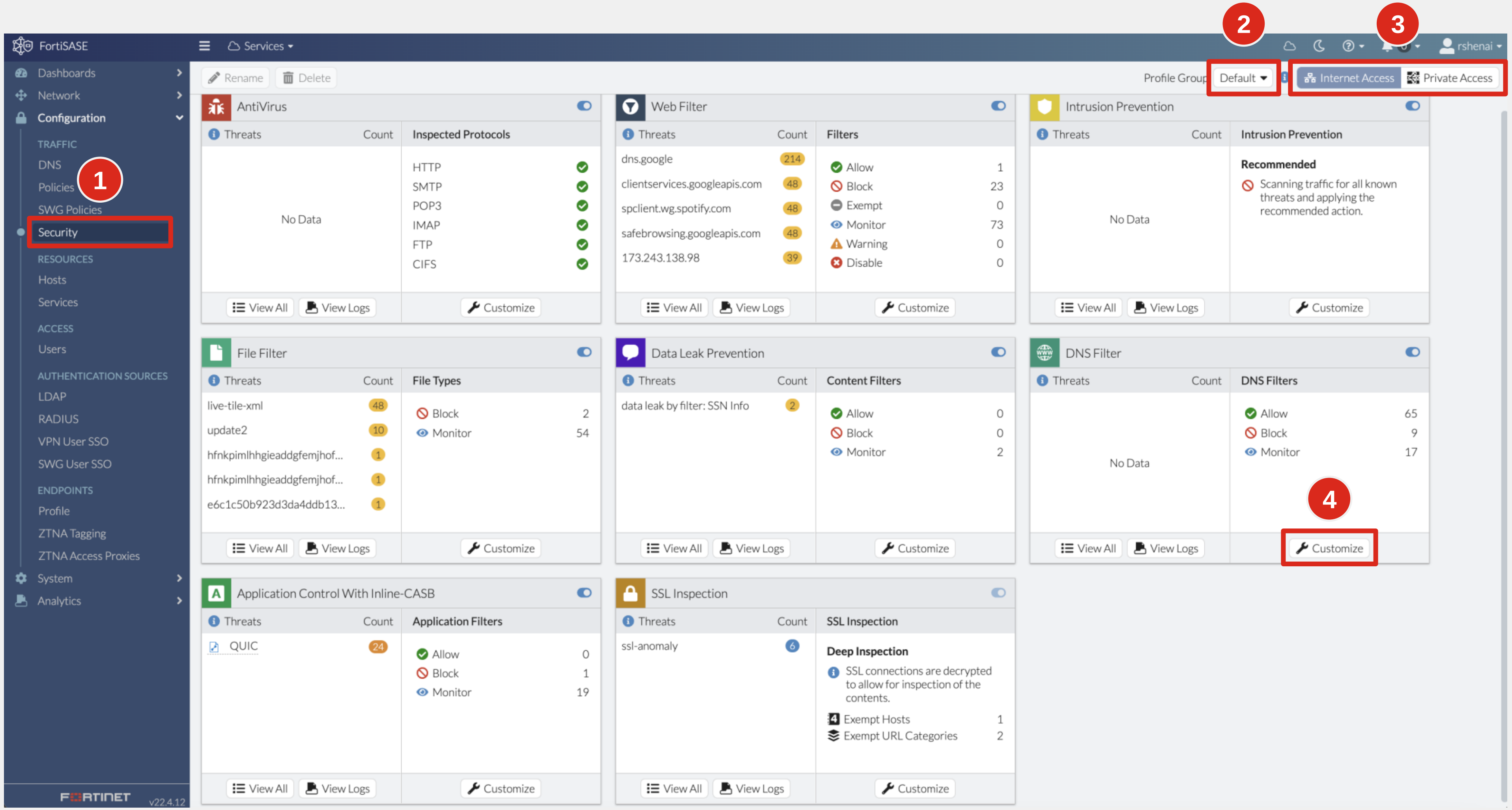
Deep inspection of web activity for threats, even when using secured HTTPS access

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

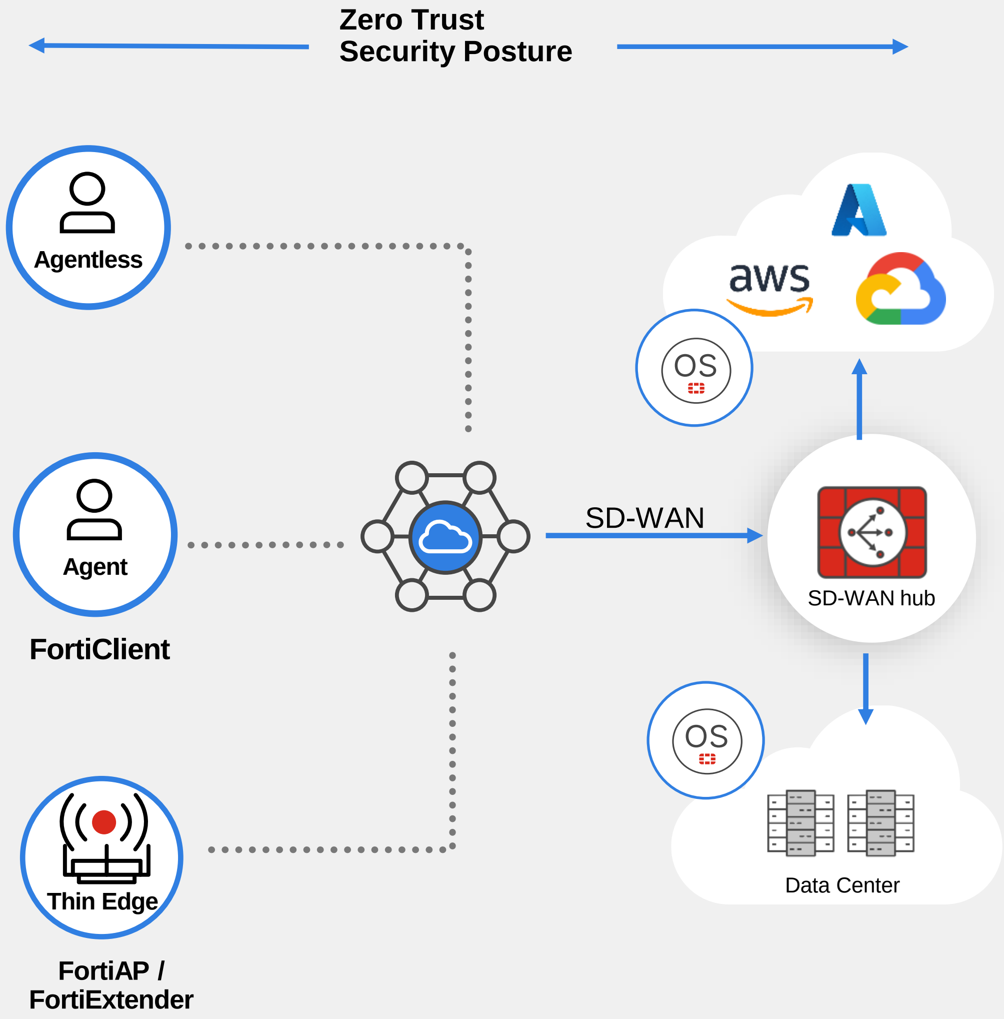
Secure anywhere access to corporate applications in datacenter and cloud with deep security inspection

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



© Fortinet Inc. All Rights Reserved.

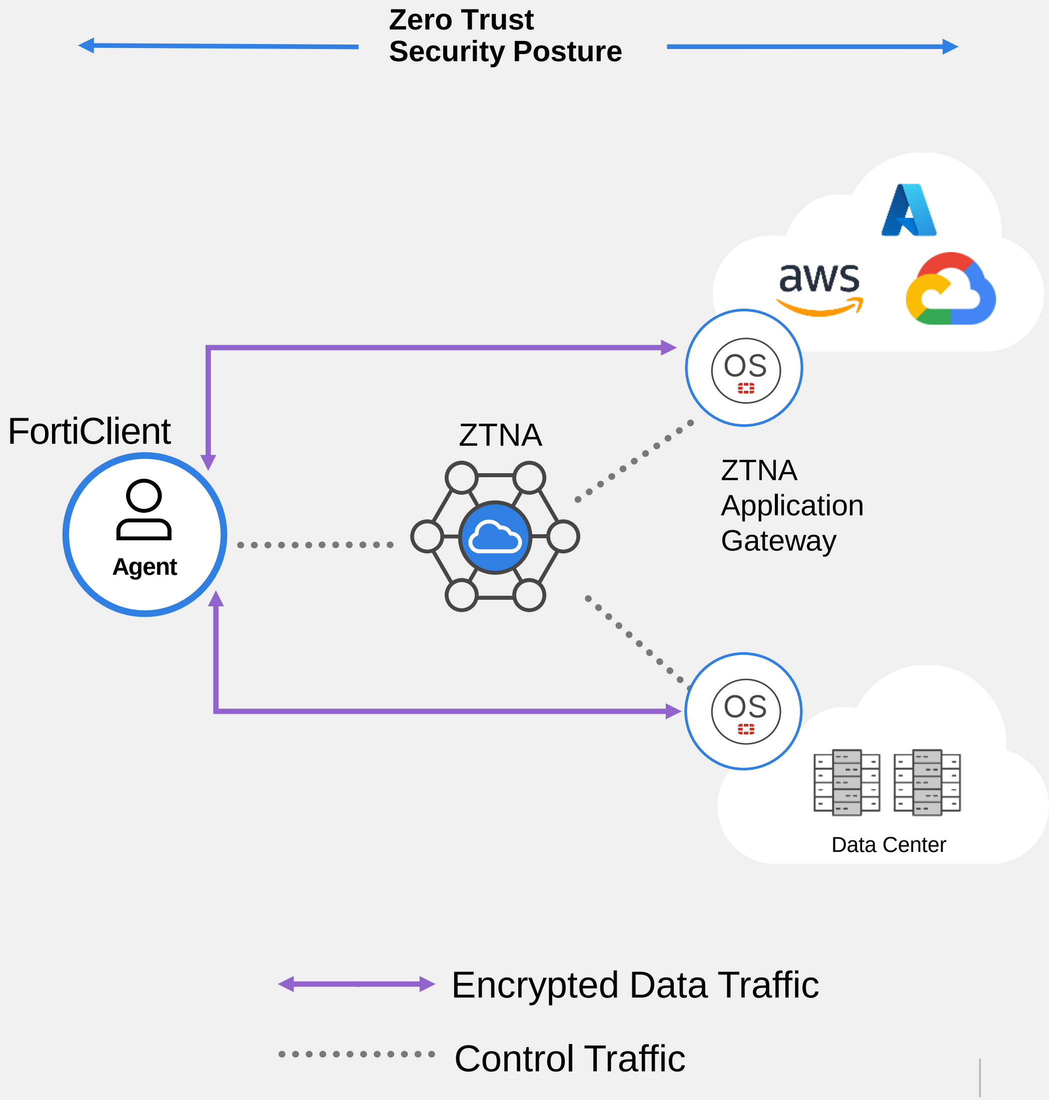
Secure Private Access with ZTNA

Cloud delivered ZTNA with FortiSASE

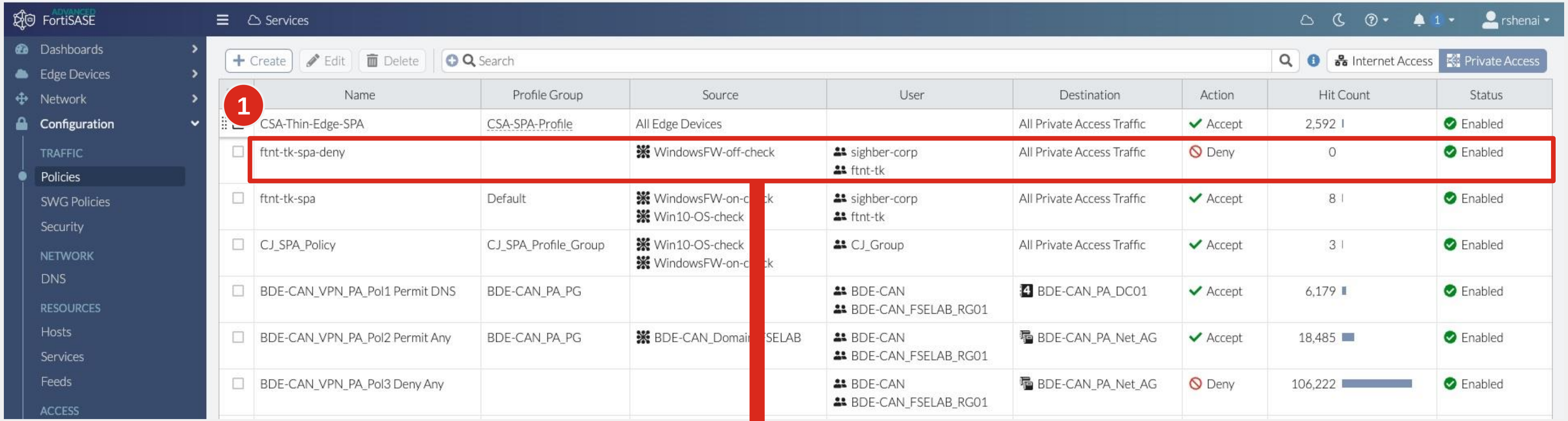
User identity and **device posture** validated for access from anywhere

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

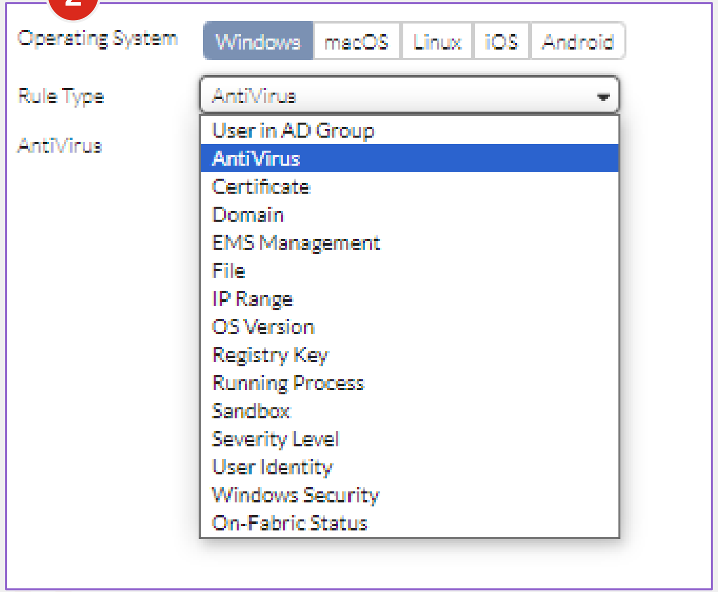
Continuous device posture re-assessment



Zero Trust security for secure application access



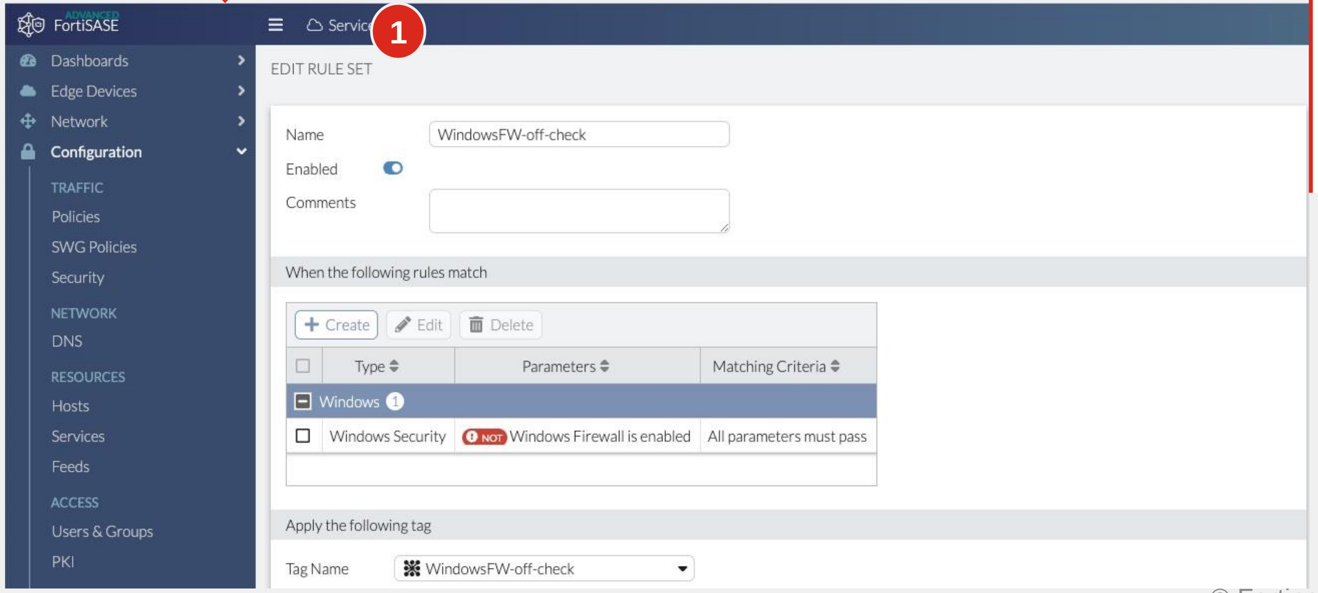
Name	Profile Group	Source	User	Destination	Action	Hit Count	Status
CSA-Thin-Edge-SPA	CSA-SPA-Profile	All Edge Devices		All Private Access Traffic	✓ Accept	2,592	Enabled
ftnt-tk-spa-deny		WindowsFW-off-check	sighber-corp ftnt-tk	All Private Access Traffic	⊘ Deny	0	Enabled
ftnt-tk-spa	Default	WindowsFW-on-check 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-check	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_Domain_FSELAB	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

Secure Private Access

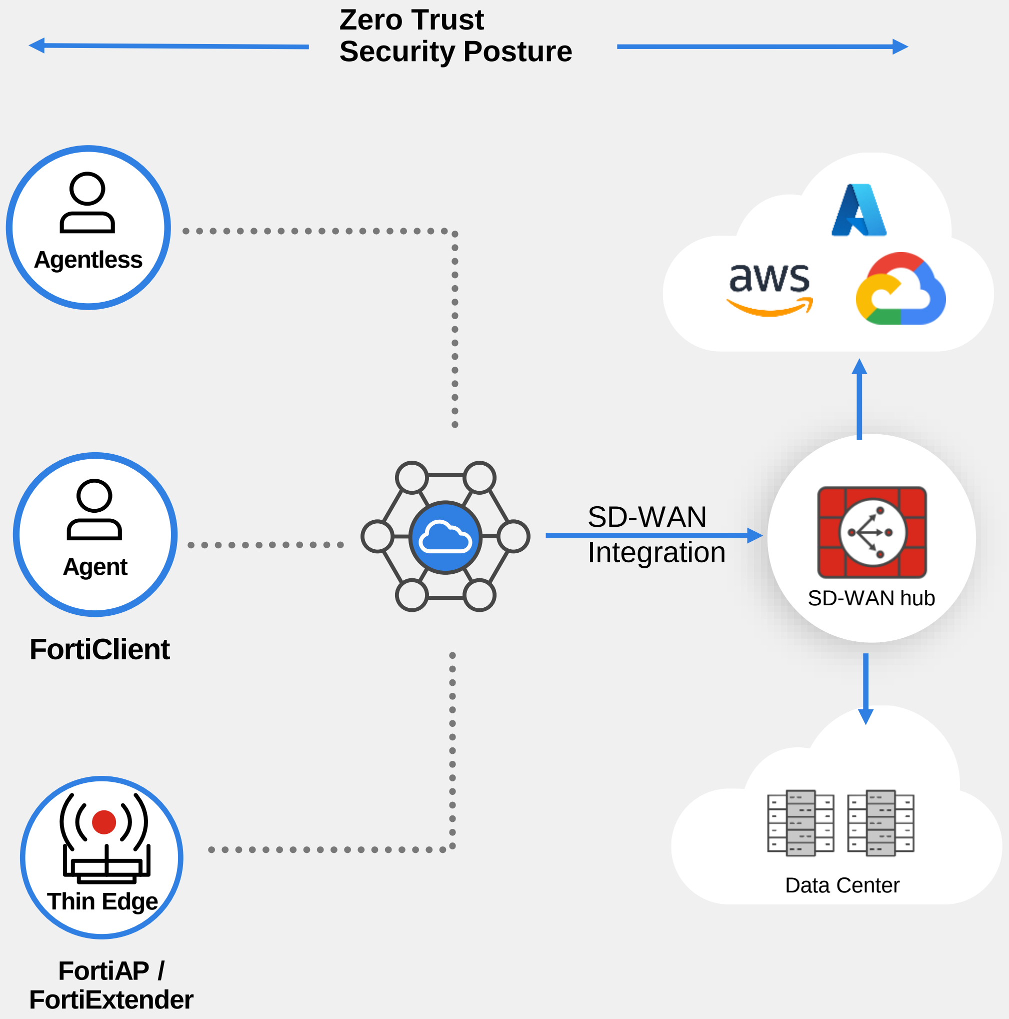
With seamless SD-WAN integration

SD-WAN Private Access

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

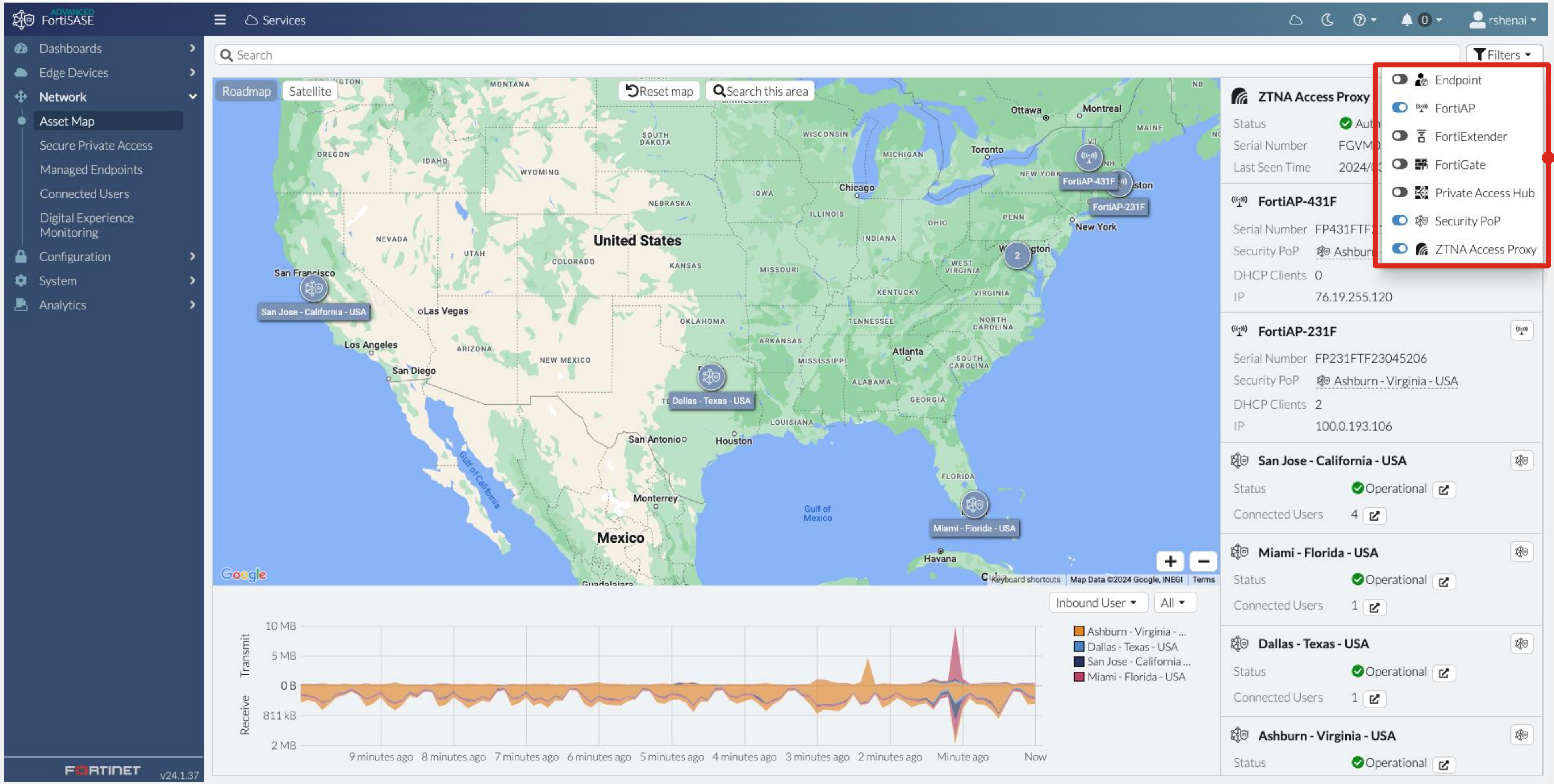
Fast access to applications using **SD-WAN** from SASE PoP to SD-WAN Hub

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



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

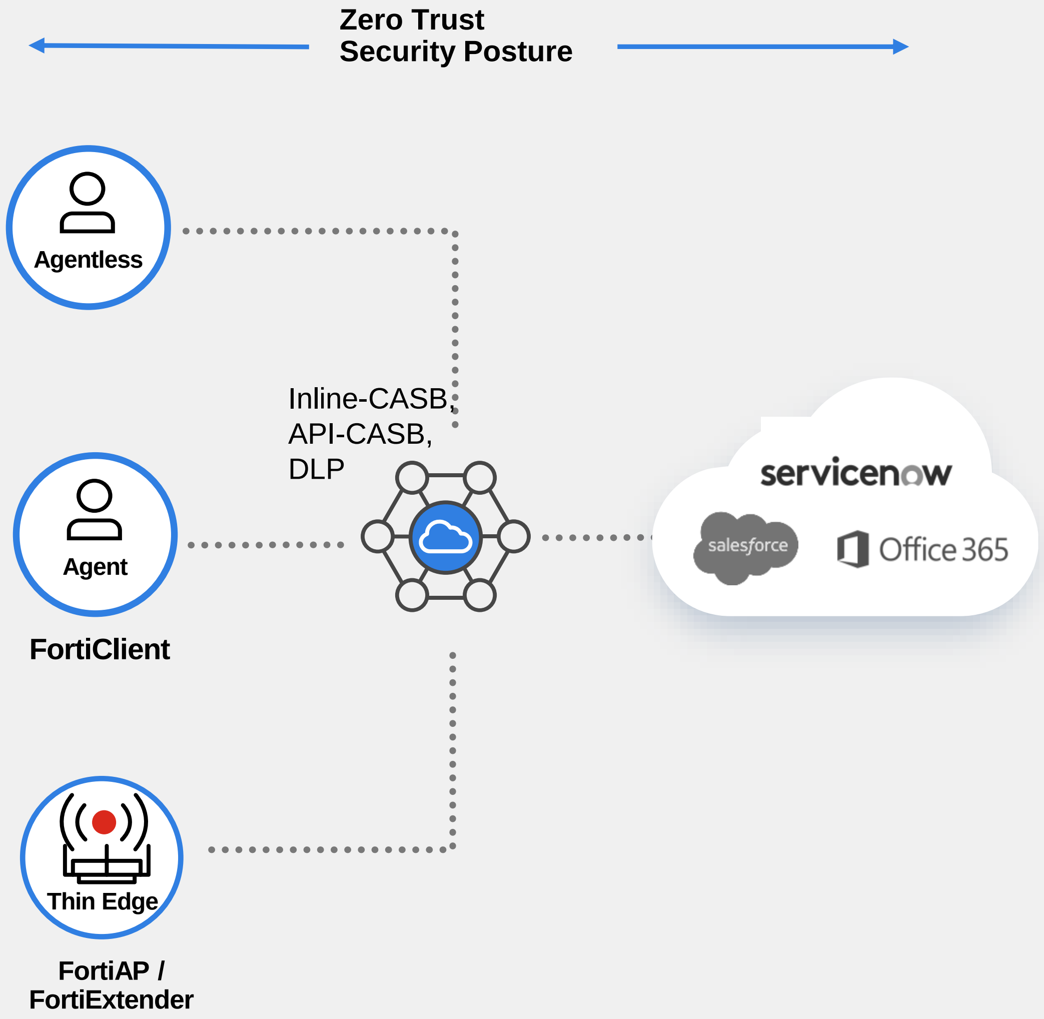
Safe Cloud Application access and blocking of malicious apps with in-line CASB feature, including Zero Trust posture checks

Deep control & view of apps content

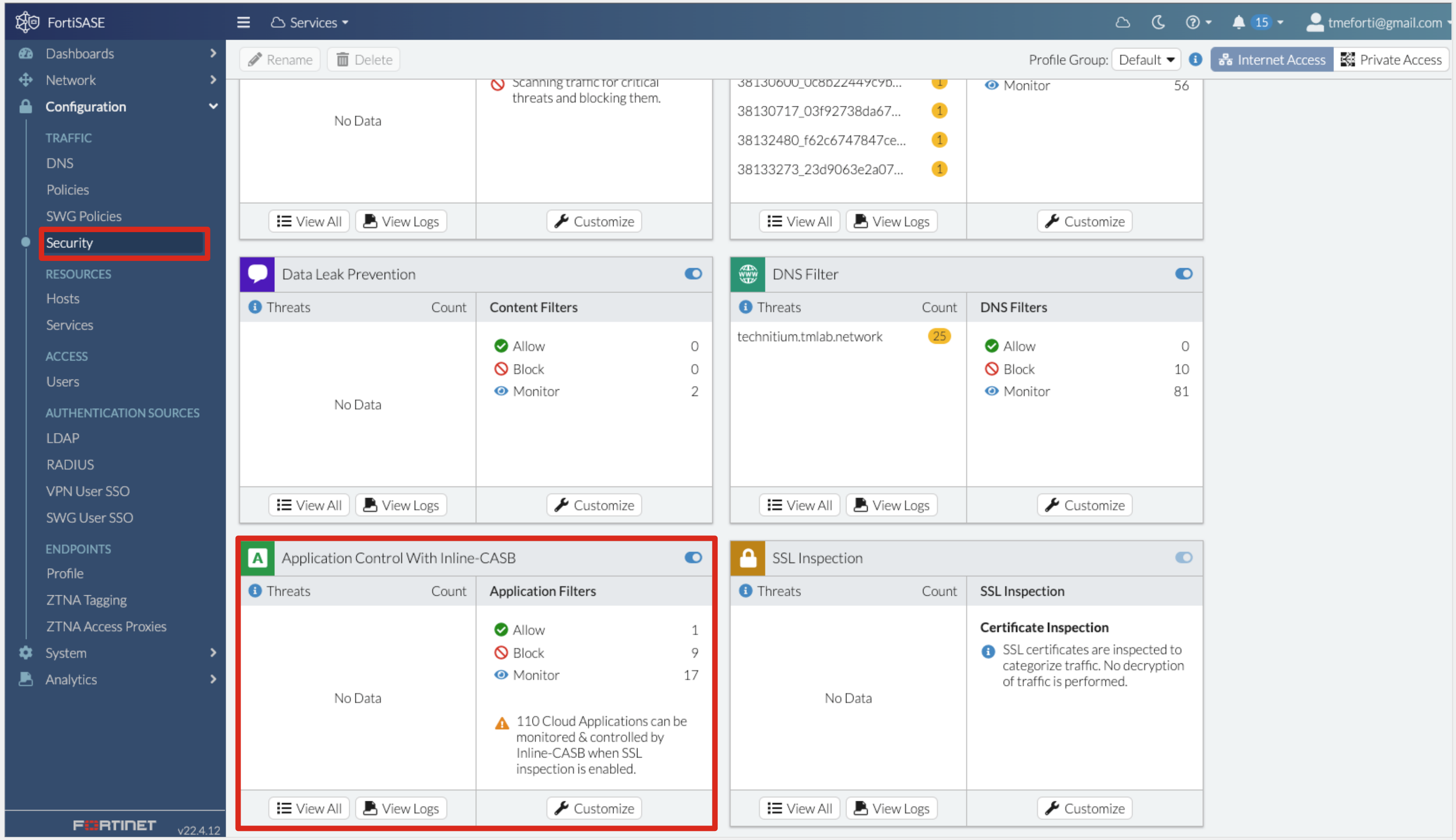
Control over app content and files with API-based CASB for enhanced security and threat detection

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



No Data

Scanning traffic for critical threats and blocking them.

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

Monitor 56

Data Leak Prevention

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

DNS Filter

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

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.

SSL Inspection

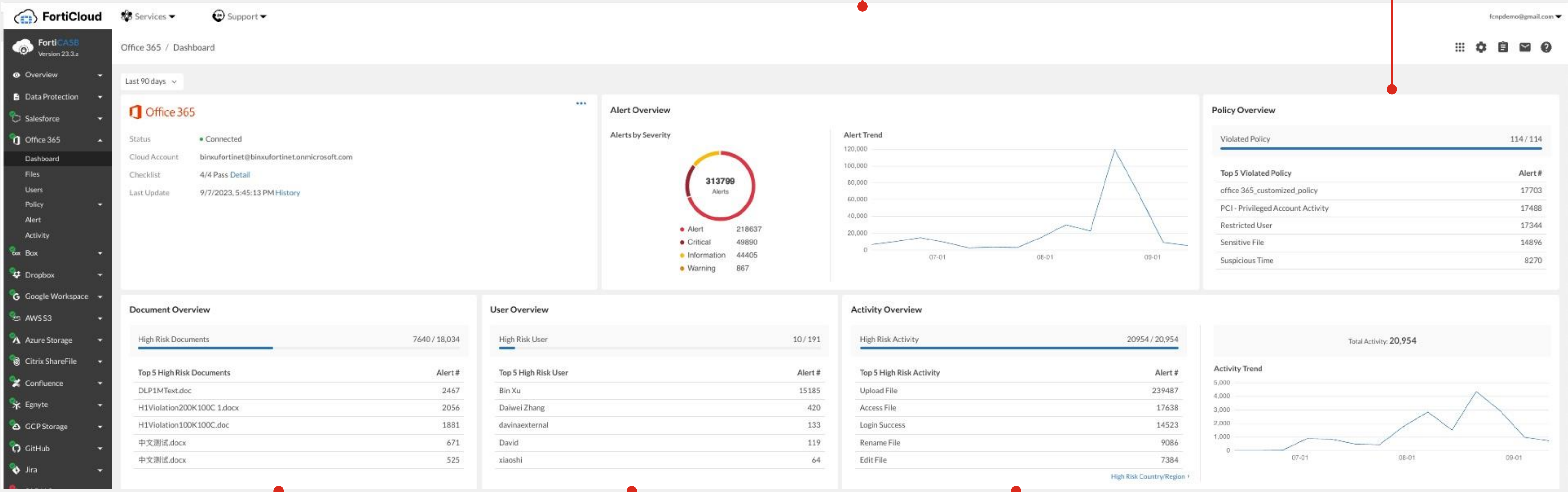
Threats	Count	SSL Inspection
No Data		**Certificate Inspection** SSL certificates are inspected to categorize traffic. No decryption of traffic is performed.

- 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

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

313799 Alerts

● 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

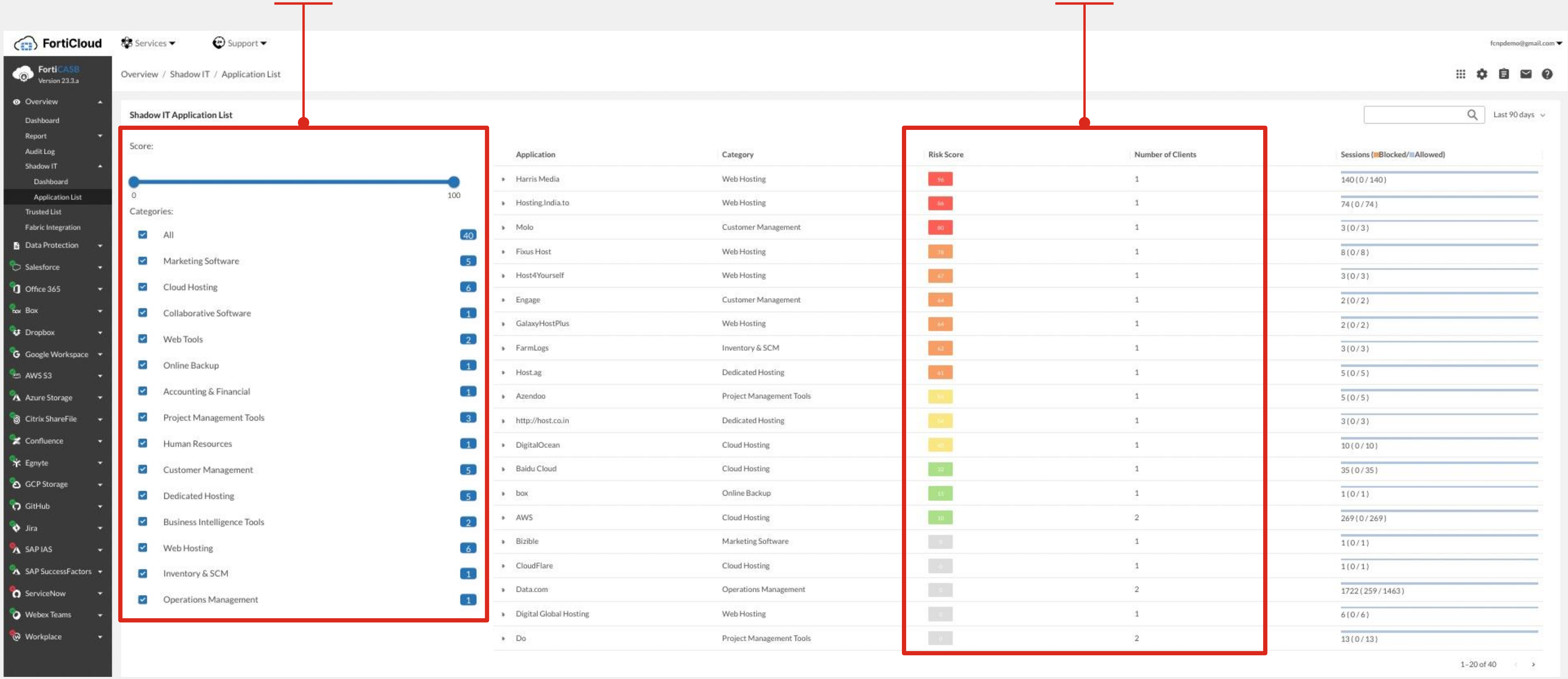
Users profiled as per Risk

Activities profiled as per Risk

Shadow IT: Application List

Filtering based on Risk score or app type

Risk score vs user breakdown



Shadow IT Application List

Score:

0 — 100

Categories:

☑	All	40
☑	Marketing Software	5
☑	Cloud Hosting	6
☑	Collaborative Software	1
☑	Web Tools	2
☑	Online Backup	1
☑	Accounting & Financial	1
☑	Project Management Tools	3
☑	Human Resources	1
☑	Customer Management	5
☑	Dedicated Hosting	5
☑	Business Intelligence Tools	2
☑	Web Hosting	6
☑	Inventory & SCM	1
☑	Operations Management	1

Application	Category	Risk Score	Number of Clients	Sessions (🟧Blocked/🟦Allowed)
Harris Media	Web Hosting	96	1	140 (0 / 140)
Hosting.India.to	Web Hosting	86	1	74 (0 / 74)
Molo	Customer Management	80	1	3 (0 / 3)
Fixus Host	Web Hosting	78	1	8 (0 / 8)
Host4Yourself	Web Hosting	67	1	3 (0 / 3)
Engage	Customer Management	64	1	2 (0 / 2)
GalaxyHostPlus	Web Hosting	64	1	2 (0 / 2)
FarmLogs	Inventory & SCM	62	1	3 (0 / 3)
Host.ag	Dedicated Hosting	61	1	5 (0 / 5)
Azendoo	Project Management Tools	54	1	5 (0 / 5)
http://host.co.in	Dedicated Hosting	54	1	3 (0 / 3)
DigitalOcean	Cloud Hosting	40	1	10 (0 / 10)
Baidu Cloud	Cloud Hosting	32	1	35 (0 / 35)
box	Online Backup	15	1	1 (0 / 1)
AWS	Cloud Hosting	10	2	269 (0 / 269)
Bizible	Marketing Software	0	1	1 (0 / 1)
CloudFlare	Cloud Hosting	0	1	1 (0 / 1)
Data.com	Operations Management	0	2	1722 (259 / 1463)
Digital Global Hosting	Web Hosting	0	1	6 (0 / 6)
Do	Project Management Tools	0	2	13 (0 / 13)

1-20 of 40

Comprehensive Data Security

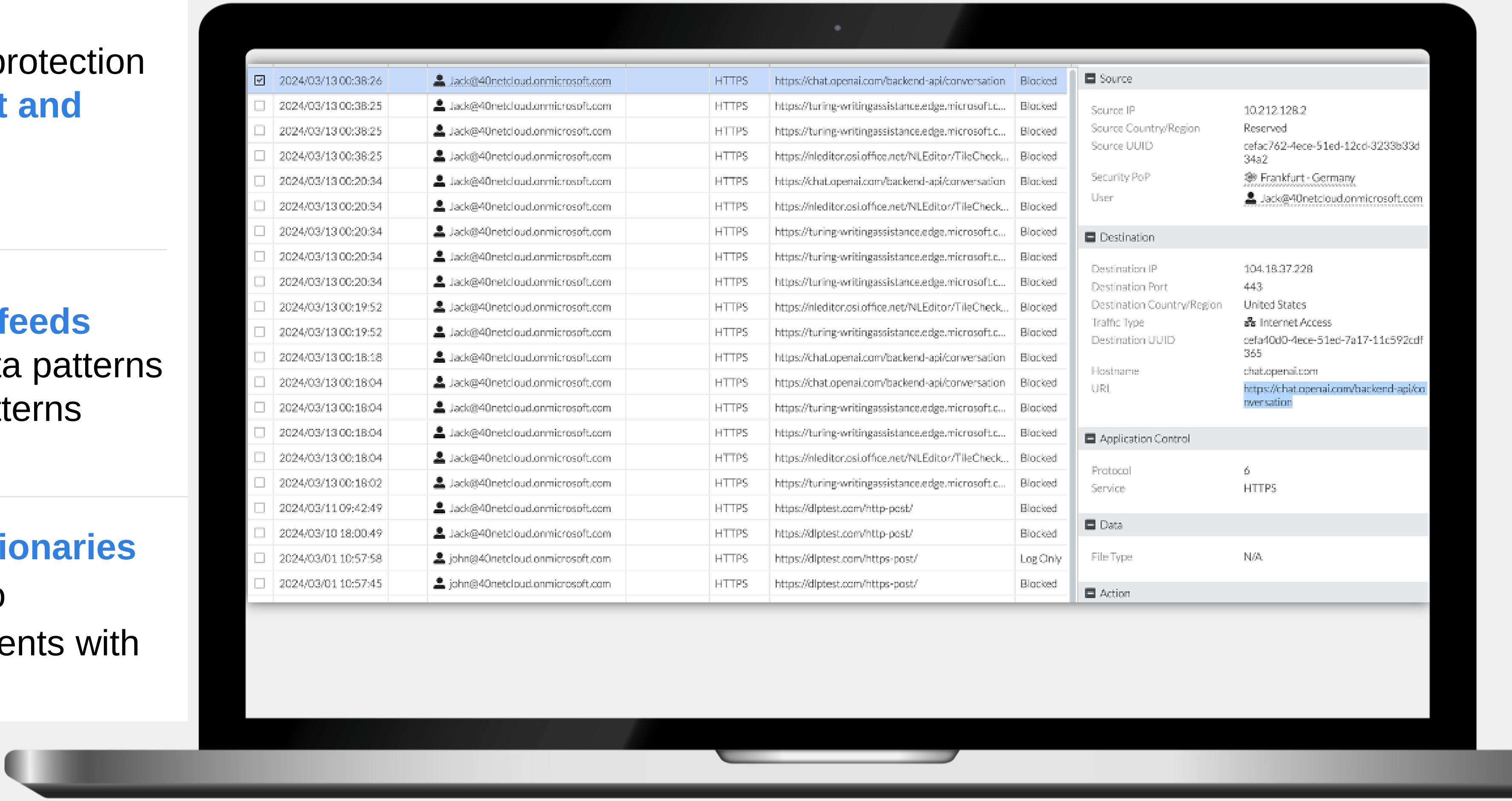
Built-in Data Leakage Protection (DLP)

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

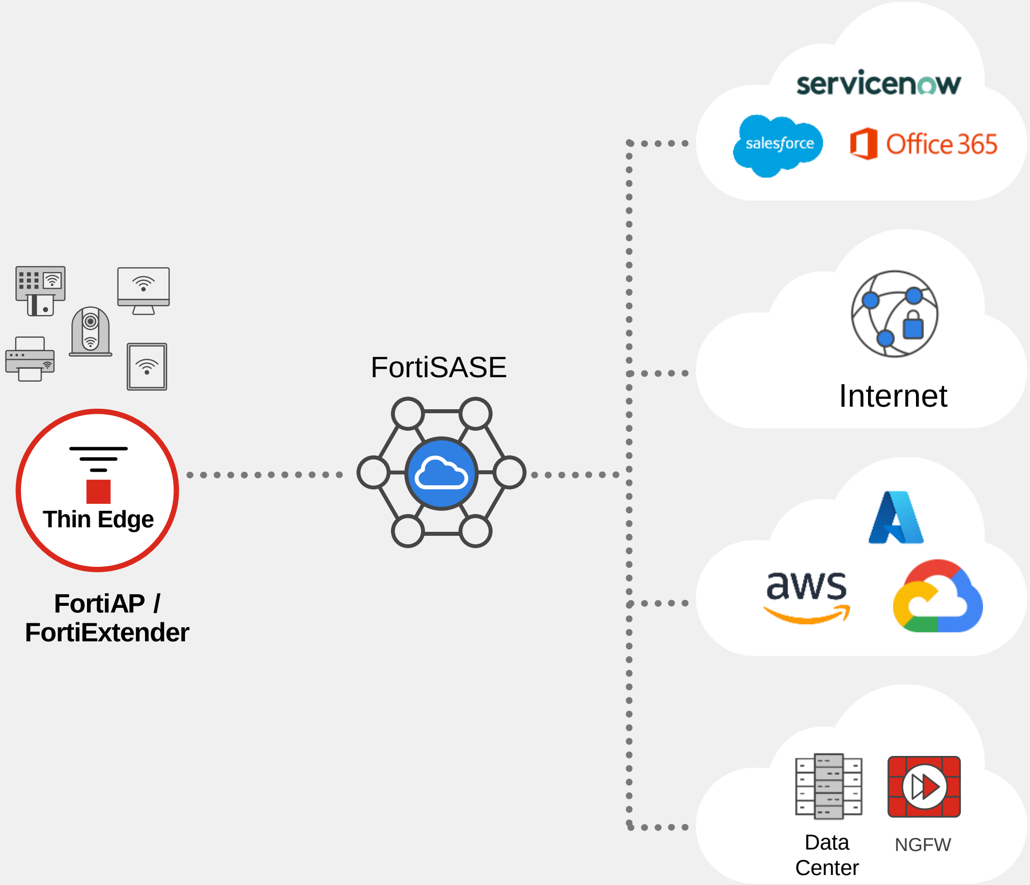
Secure thin edge locations that don't have on-prem firewall to block ransomware and malware

Secure Agentless Access from IoT

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

Cloud delivered Management

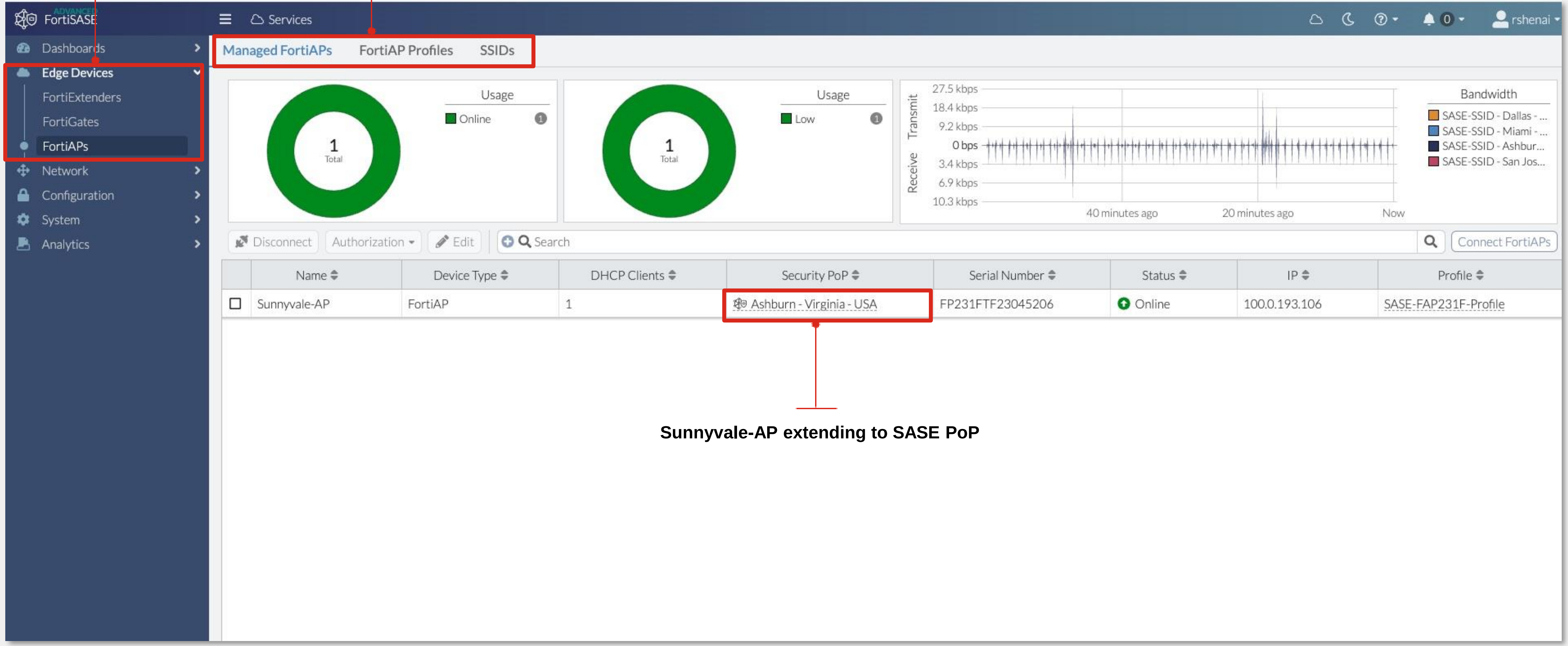
Cloud delivered management of FortiAP and FortiExtender with zero-touch provisioning support



FortiSASE Cloud Delivered Management for Thin Edge

Streamlined Management

Single pane to manage



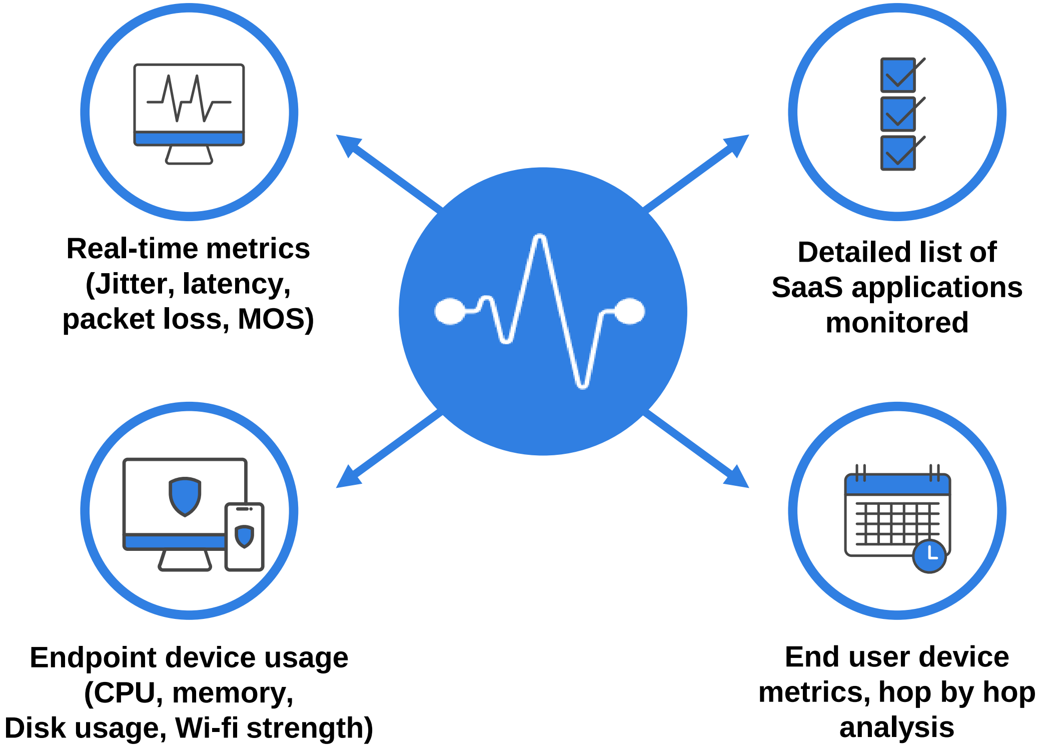
	Name	Device Type	DHCP Clients	Security PoP	Serial Number	Status	IP	Profile
□	Sunnyvale-AP	FortiAP	1	Ashburn - Virginia - USA	FP231FTF23045206	Online	100.0.193.106	SASE-FAP231F-Profile

Sunnyvale-AP extending to SASE PoP

Advanced features

End-to-End Digital Experience Monitoring

Comprehensive visibility | Metrics and alerts correlation | Proactive response

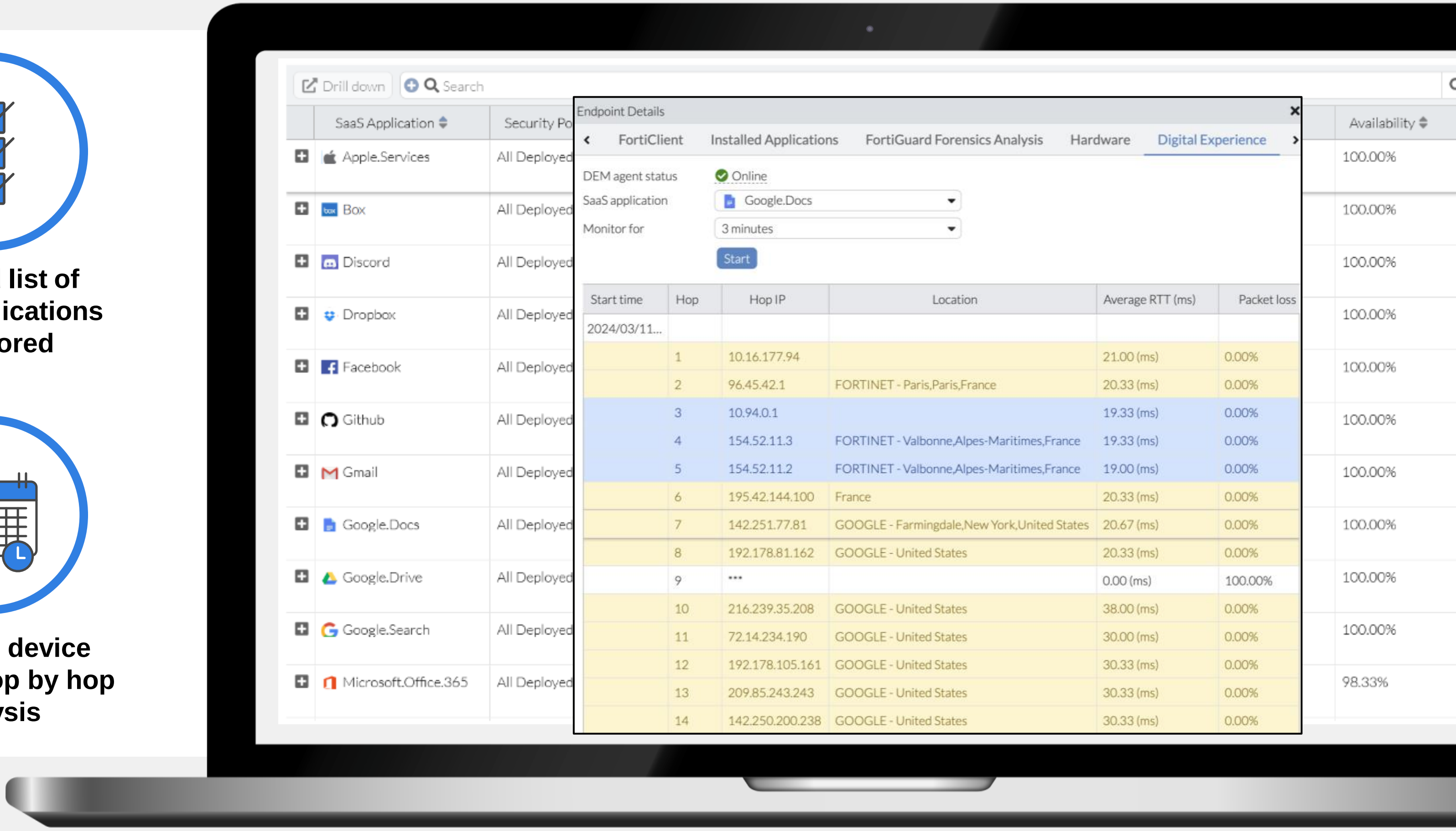


Real-time metrics (Jitter, latency, packet loss, MOS)

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!

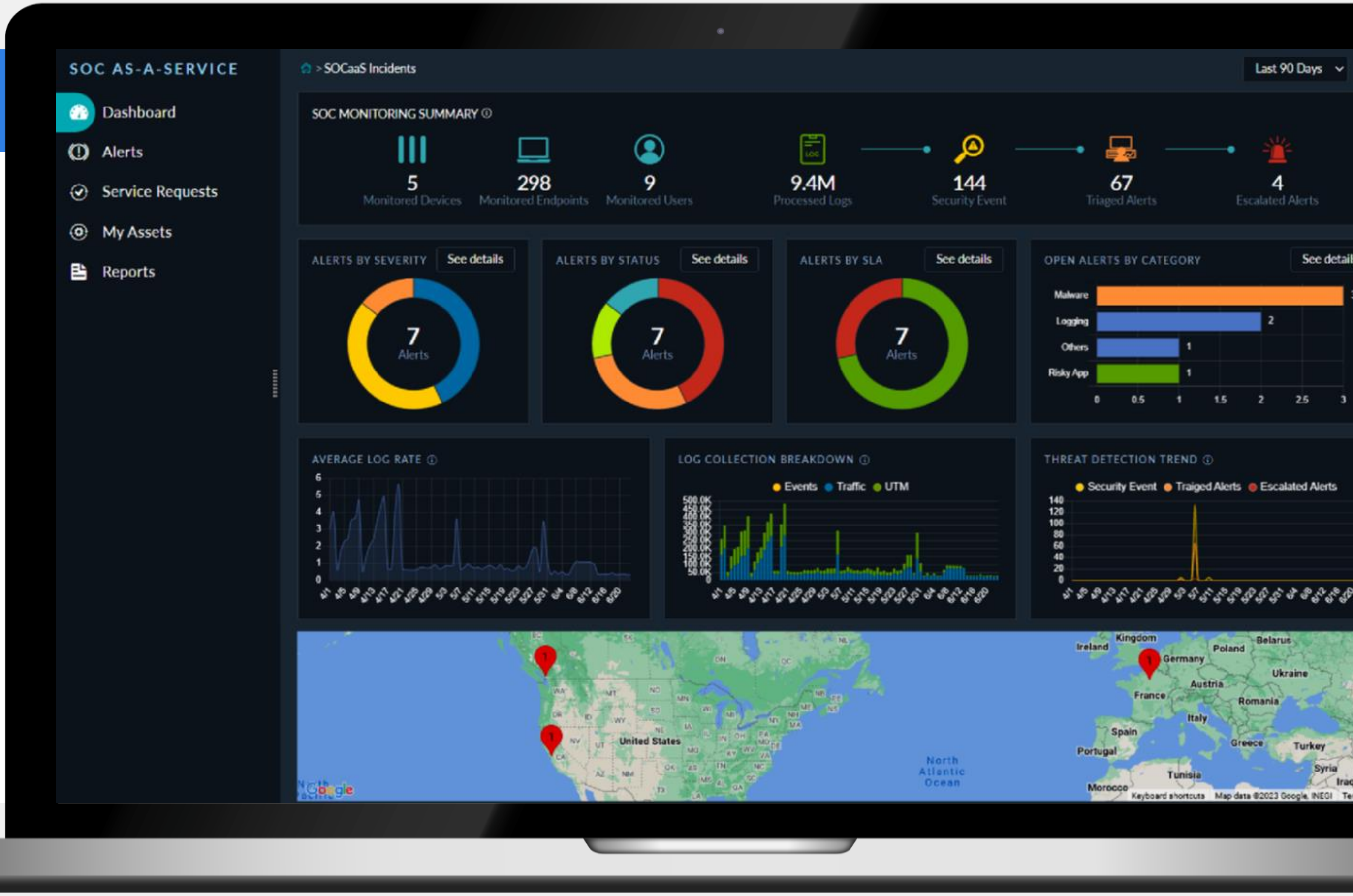
24x7 Human based Monitoring and analysis with weekly summary reports, alerts and notifications

Respond: Act Fast

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

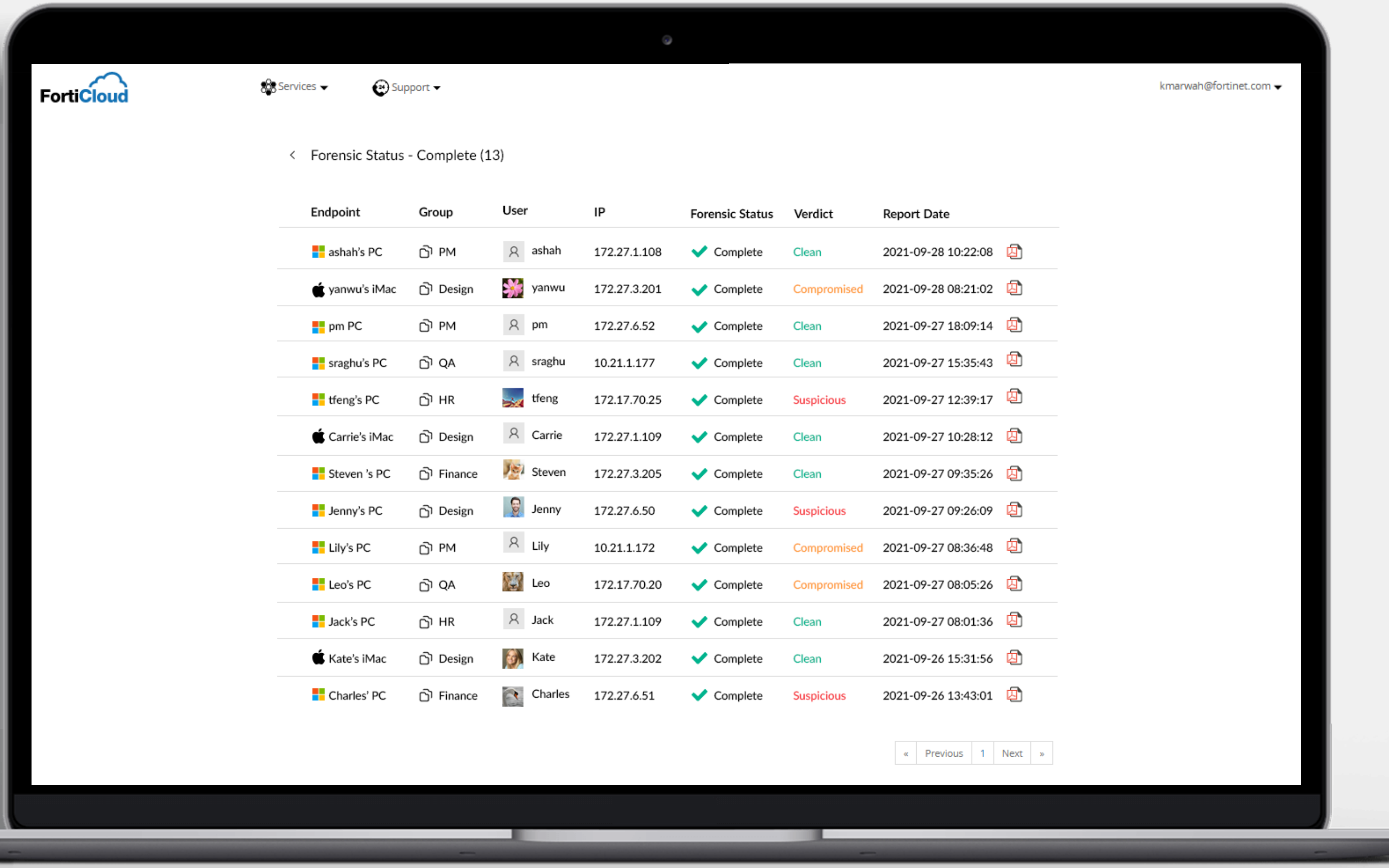
Improve: Maximize Investment

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

Business outcomes & Benefits

Secure Access to Any Application for Any User

UNIFIED SECURE ACCESS FOR HYBRID WORKERS

The Fortinet secure access service edge (SASE) solution enables secure access to the web, cloud, and applications for the hybrid workforce, while simplifying operations and universal Zero Trust

CONSISTENT SECURITY

Eliminated gaps in security for remote users by providing same level of security as in office

50% Reduction in man hours for operations with consistent security

Reducing Cost

Reduced TCO and simplified operations using single console to centrally manage all components

68% Reduction in TCO with consolidation

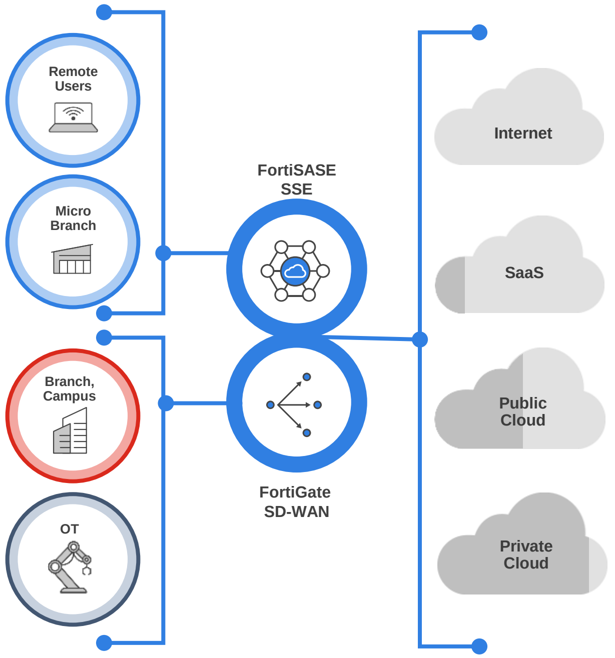
BETTER USER EXPERIENCE

Improved user and guest experience with accessing applications

10x Improvement in performance

Unified SASE

Unified SASE Secures Access and Protects Networks, Applications, and Data On Any Cloud



Why Fortinet Unified SASE?

1

FortiOS Powered Convergence

OS

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

Why now, next Steps

1

SASE & ZTNA are Facts:
Read Docs, start now

2

Talk with us or with your Partner:
It’s time to move. SASE is easy
but ZTNA needs time!

3

Seeing is believing
See a Demo

FORTINET®