FortiSASE. Побудова IT інфраструктури та безпеки сервісів без датацентрів

Євгеній Таран, Systems Engineer

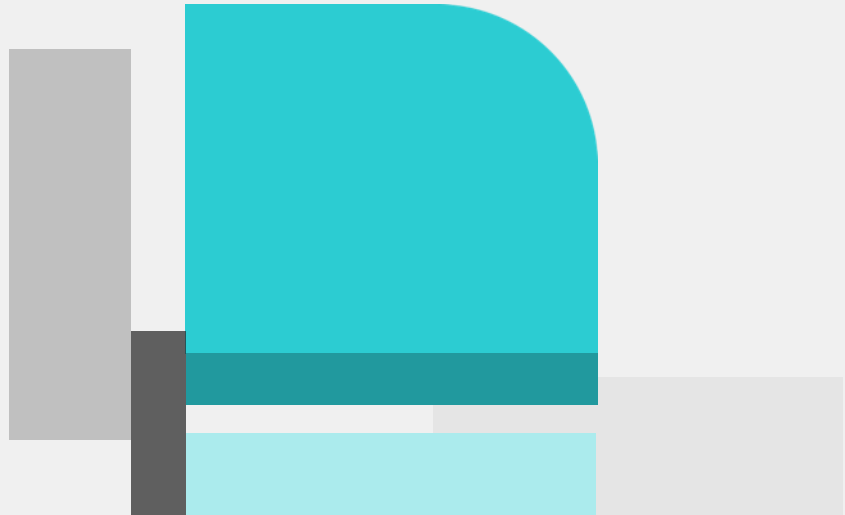
ytaran@fortinet.com

Таран Євгеній

- 15+ років в IT
- останні 9 років будую/модернізую IT інфраструктури та змушую веб сервіси працювати «як має бути» ☺
- IT системи міжнародних заходів (спортивні змагання, вибори тощо)
- Досвід роботи в 10 країнах регіону
- Fortinet NSE 7 і багато іншого

P.S. Це моя друга кібервійна…

Поява SASE рішень та їх сутність



Сучасні тенденції сервісів та їх користувачів

Робота звідусіль

84%

Джерело 1:
2023 Forbes Remote Work Trends

Сервіси всюди

125+

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

Консолідація IT

75%

Джерело 3:
2022 Gartner CISO Survey and infographics

Основа Zero Trust

Ніколи не довіряйте - завжди перевіряйте

- Доступ до необхідних сервісів на основі авторизації
- Інспекція трафіку та ПК
- Постійний моніторинг з коригуванням доступу/перевірок

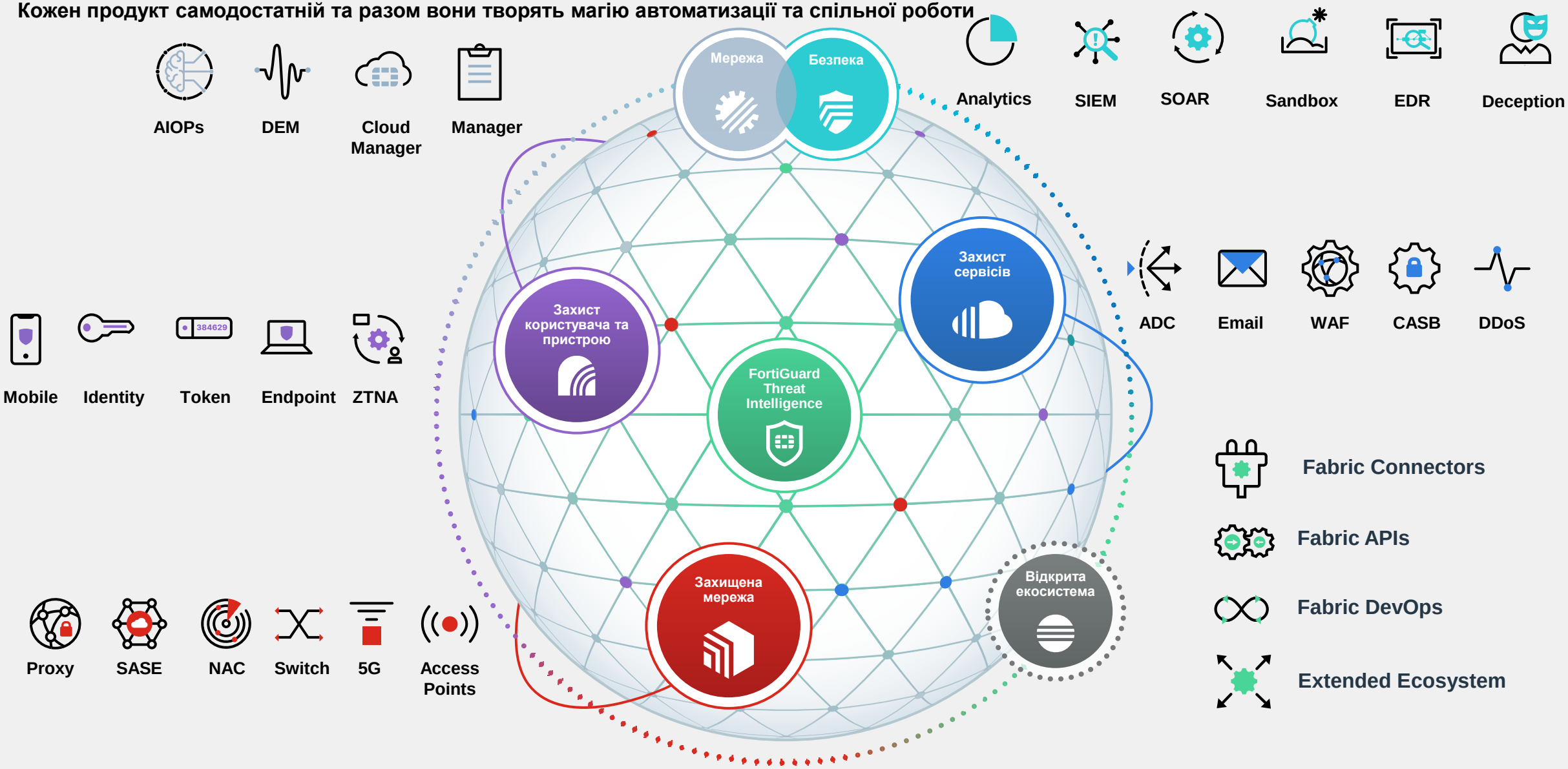
Сучасні реалії

Сучасні реалії

- Додатки різних типів
- Співробітники працюють звідусіль
- Непідконтрольні власні пристрої співробітників
- Все більше різних пристроїв
- Автоматизовані атаки
- Багато виробників
- Брак спеціалістів

Fortinet Security Fabric

Кожен продукт самодостатній та разом вони творять магію автоматизації та спільної роботи



Етап 1: Класична інфраструктура

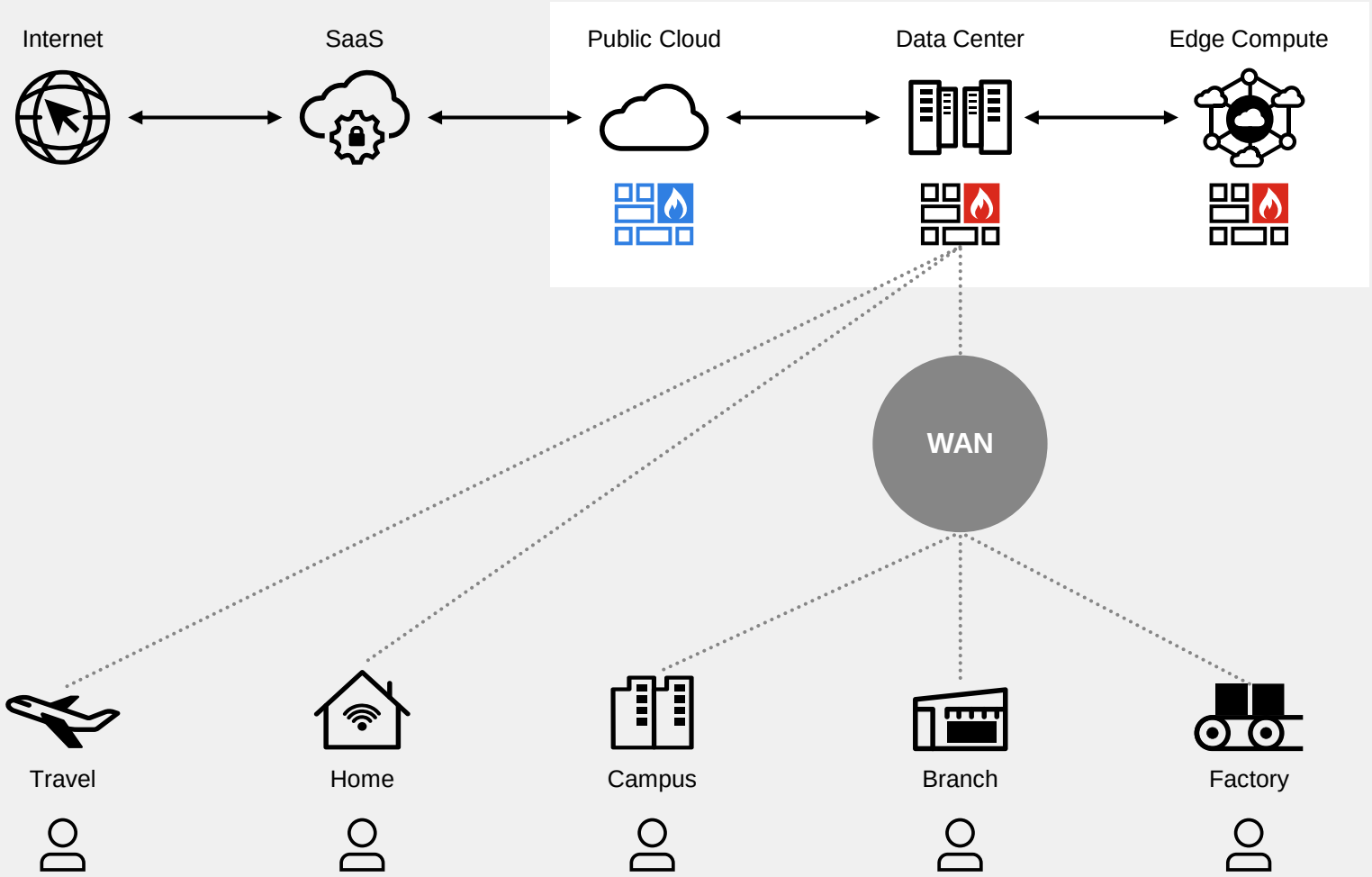
Сегментована

З захищеними сервісами

З захищеним інтернетом

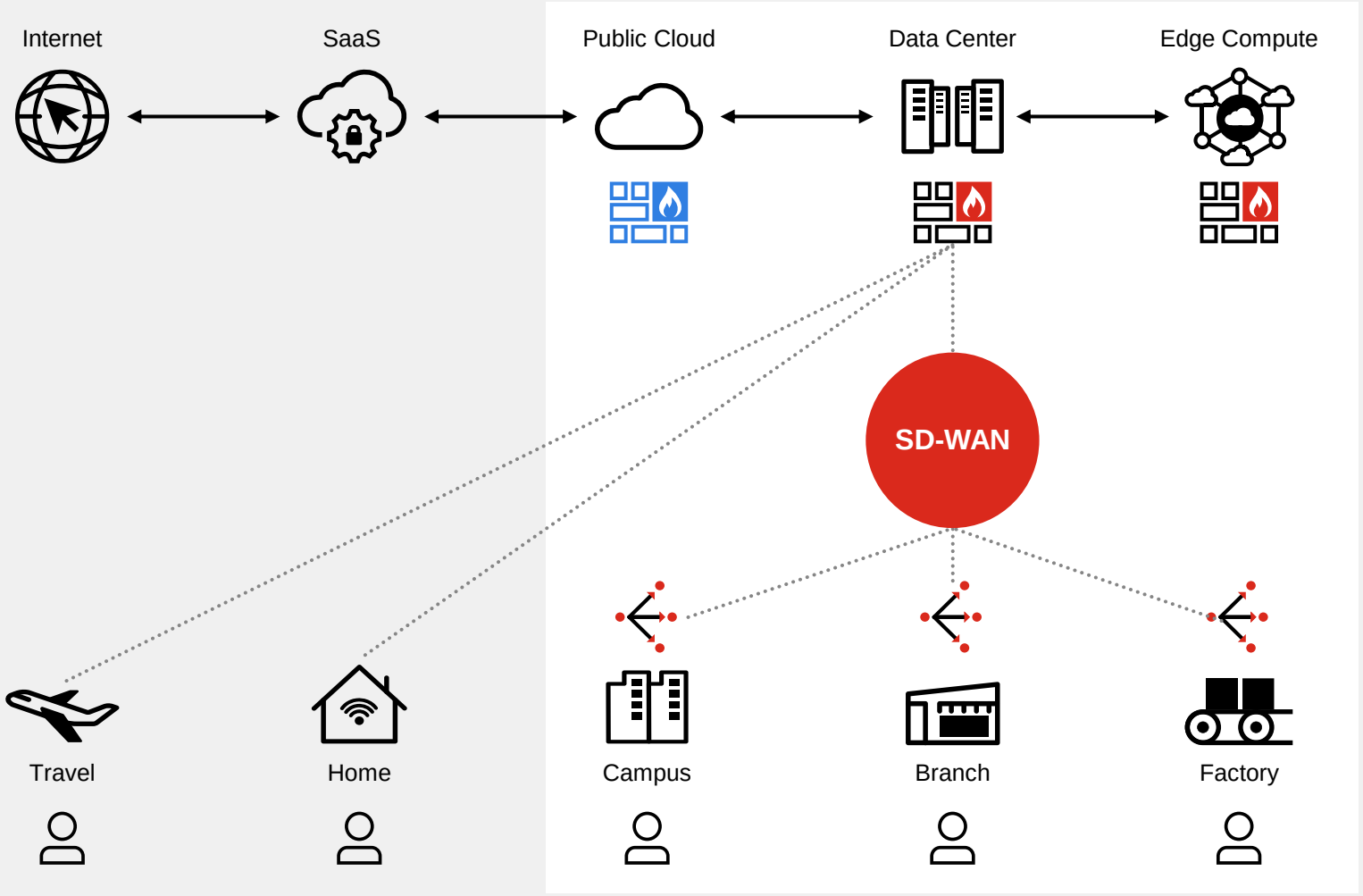
Розшифровка трафіку

VPN



Етап 2: Додаємо можливості SD-WAN

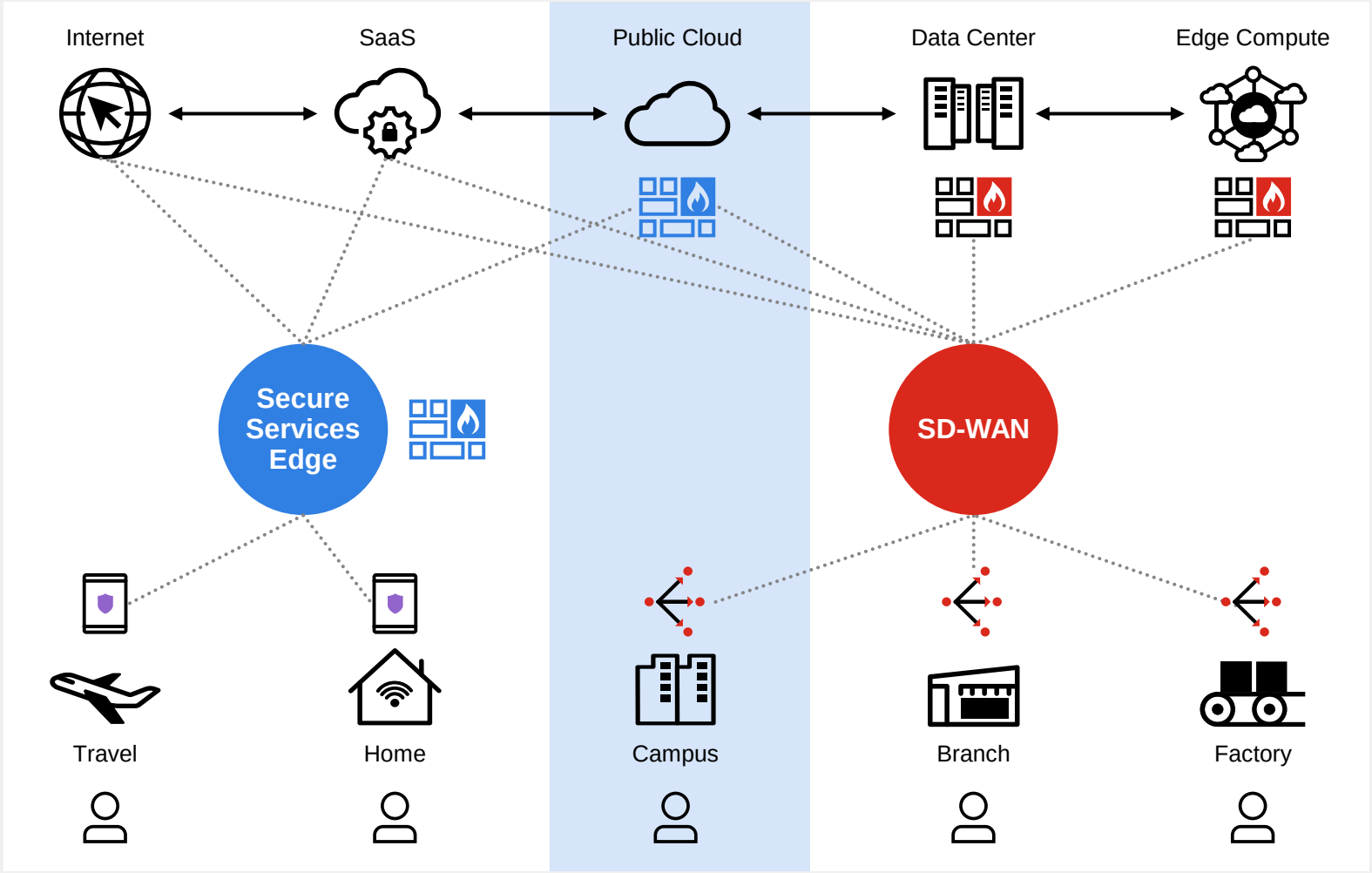
- Динамічне керування трафіком
- Пріорітезація на основі сервісу
- Висока доступність
- Підтримка бездротових каналів зв'язку в якості резерву
- Контроль швидкості та якості



Етап 3: Користувачі що працюють віддалено

Віддалені користувачі переходять на SASE Cloud

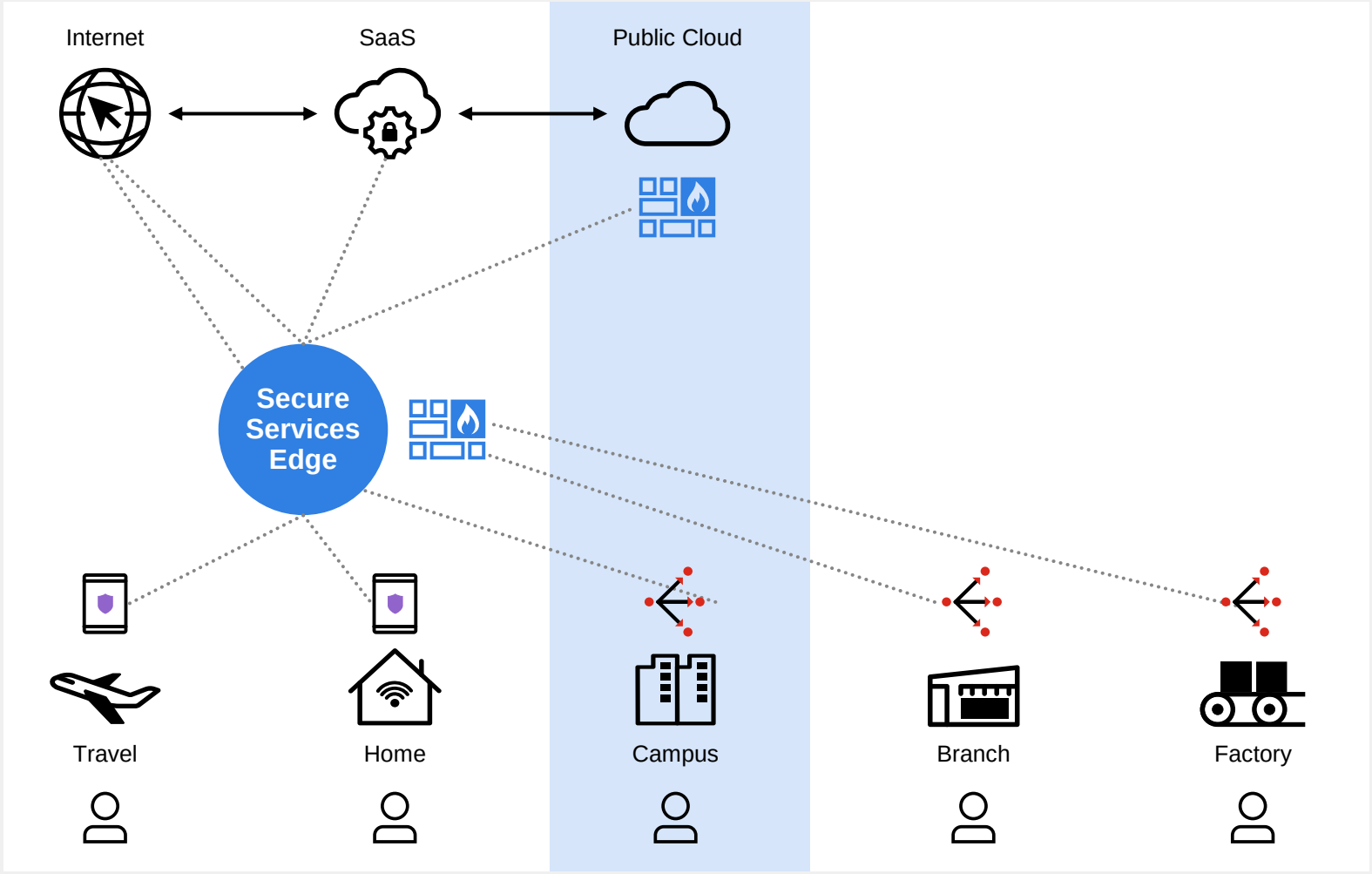
- FWaaS
- SWGaaS
- CASB



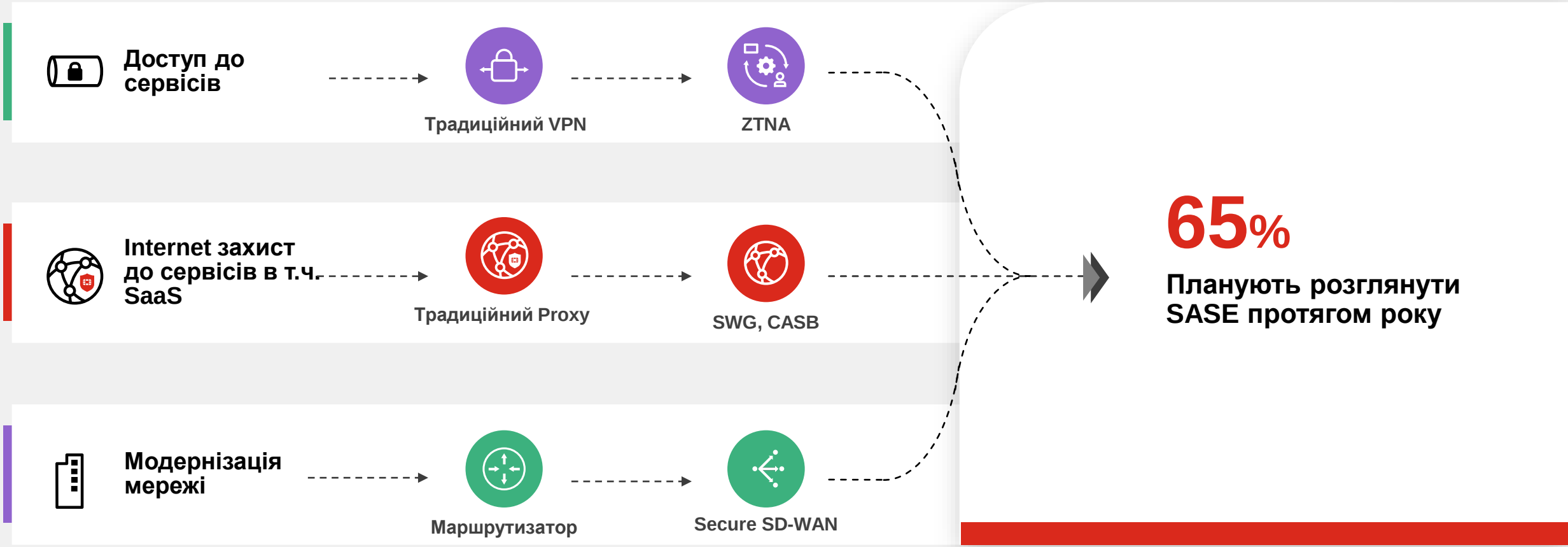
Етап 4: Відмова від локального ДЦ

Весь трафік обробляється та термінується в хмарі

Безпека забезпечується SASE хмарою у зв'язці з наземним обладнання що лишилась



Основні задачі для SASE



SASE як основа для безпечного доступ

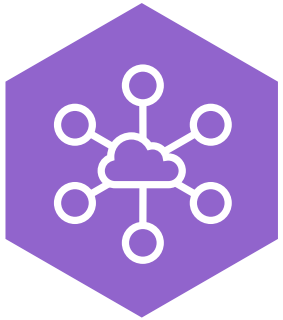
Основна ідея

Zero Trust для всіх

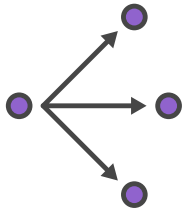
Архітектура

Secure Access Service Edge (SASE)

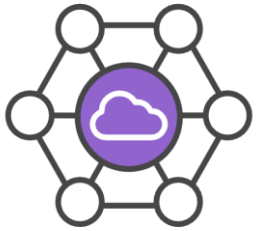
Можливості



Єдина мережа



SD-WAN



SSE

SWG/Firewall

ZTNA

CASB

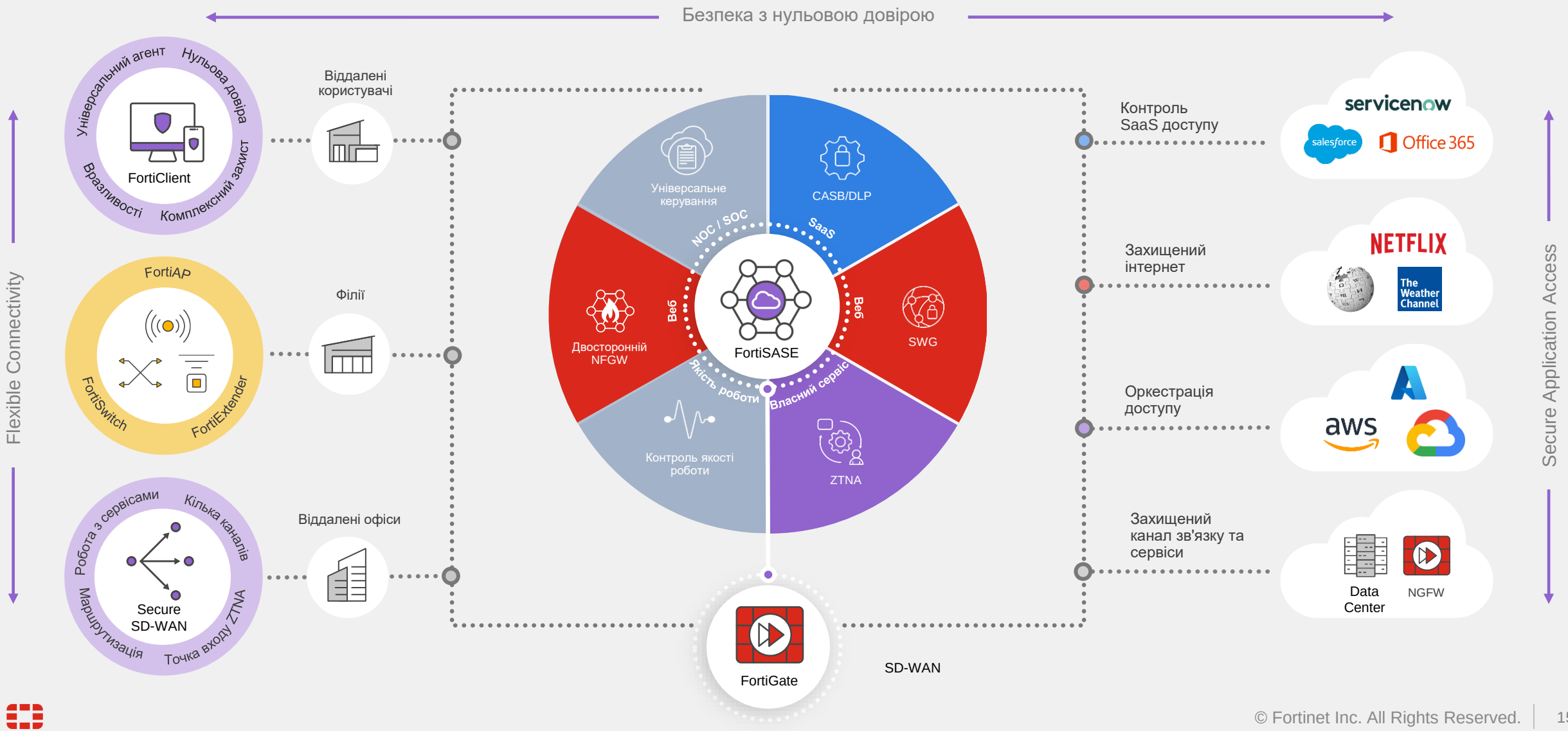
Результат

Зручний та безпечний доступ з контролем якості та безпекою

Компоненти SASE

Fortinet Universal SASE

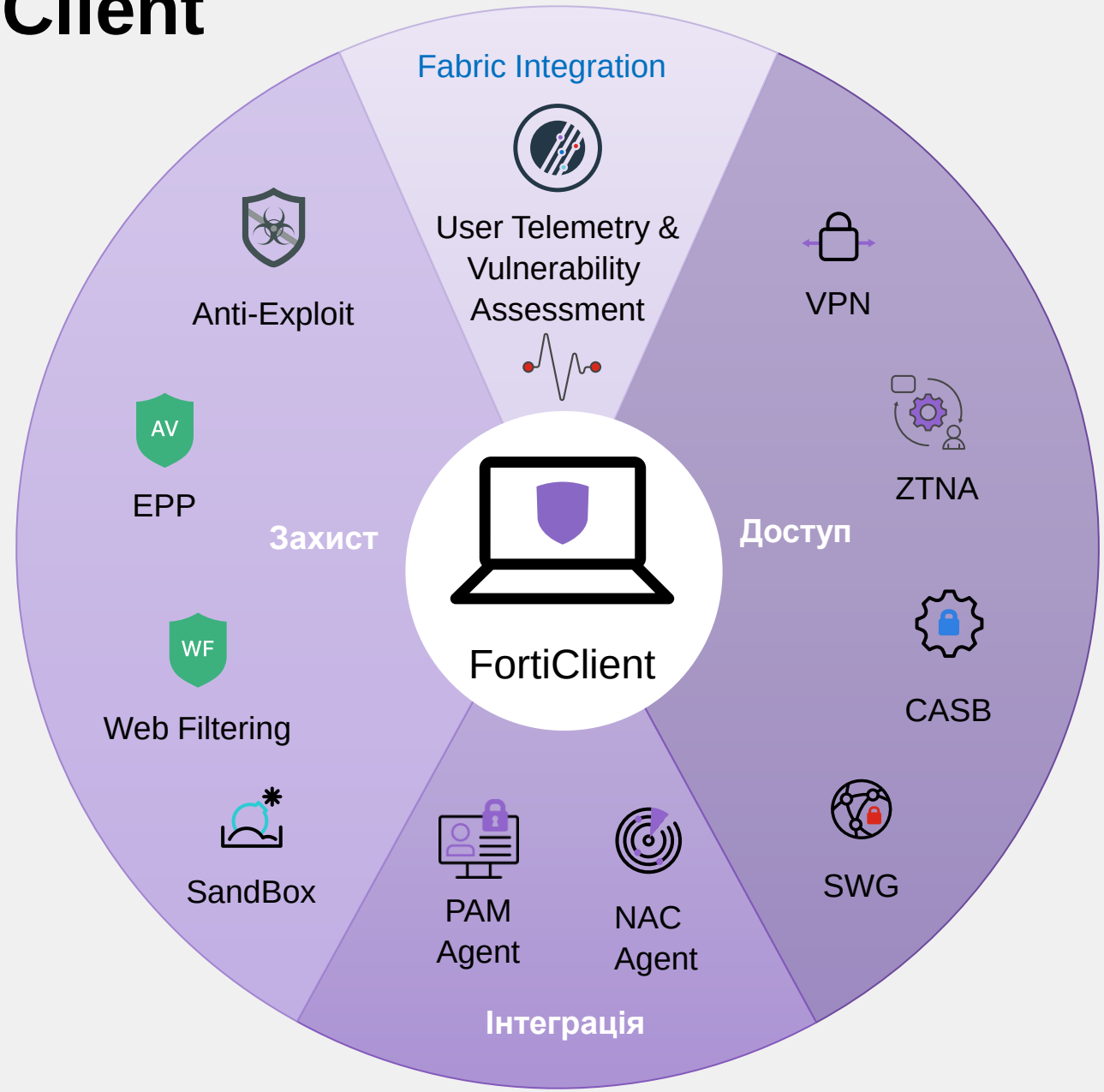
Перевірена безпека та зв’язок усюди



Уніфікований агент - FortiClient

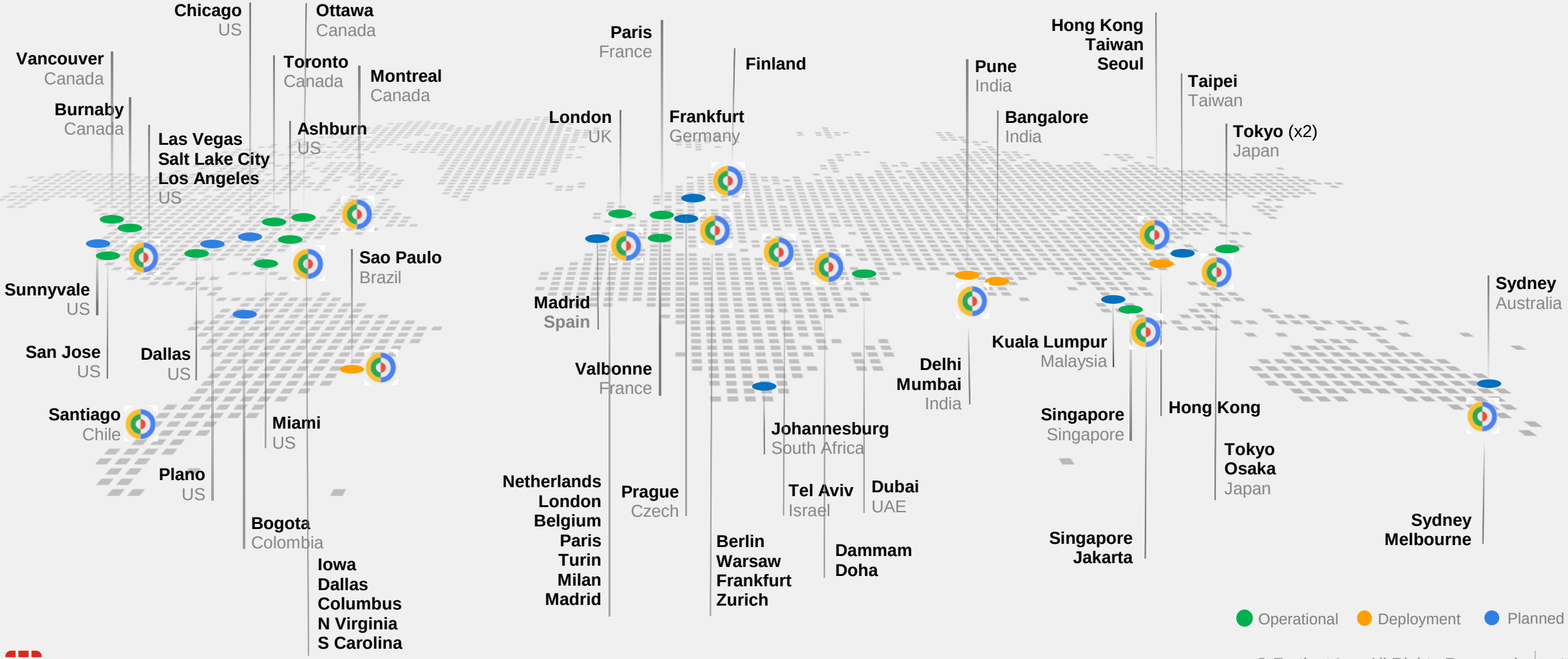
Один агент для всього*

- Єдиний агент для:
  - Доступу (ZTNA, VPN)
  - Захисту ПК (EPP)
  - SASE
  - Digital Experience (DEM)
  - Fabric Support (PAM, NAC, FortiWeb)

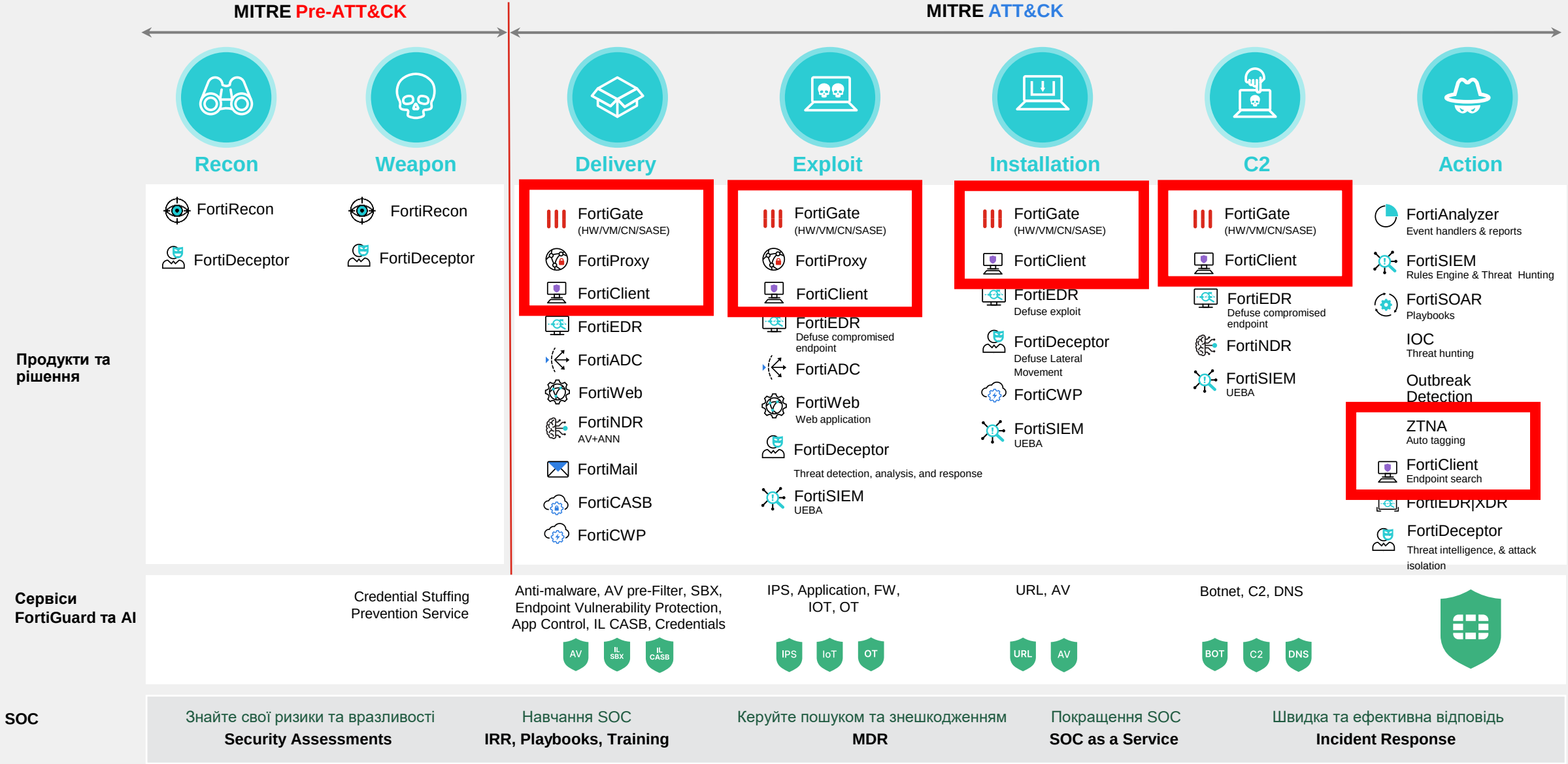


Точки присутності

Глобально | **90+ локацій** | **Безпека як сервіс** | **Низькі затримки з високим SLA**



Комплексний підхід до безпеки



Кілька прикладів використання

Безпечний Інтернет для співробітників

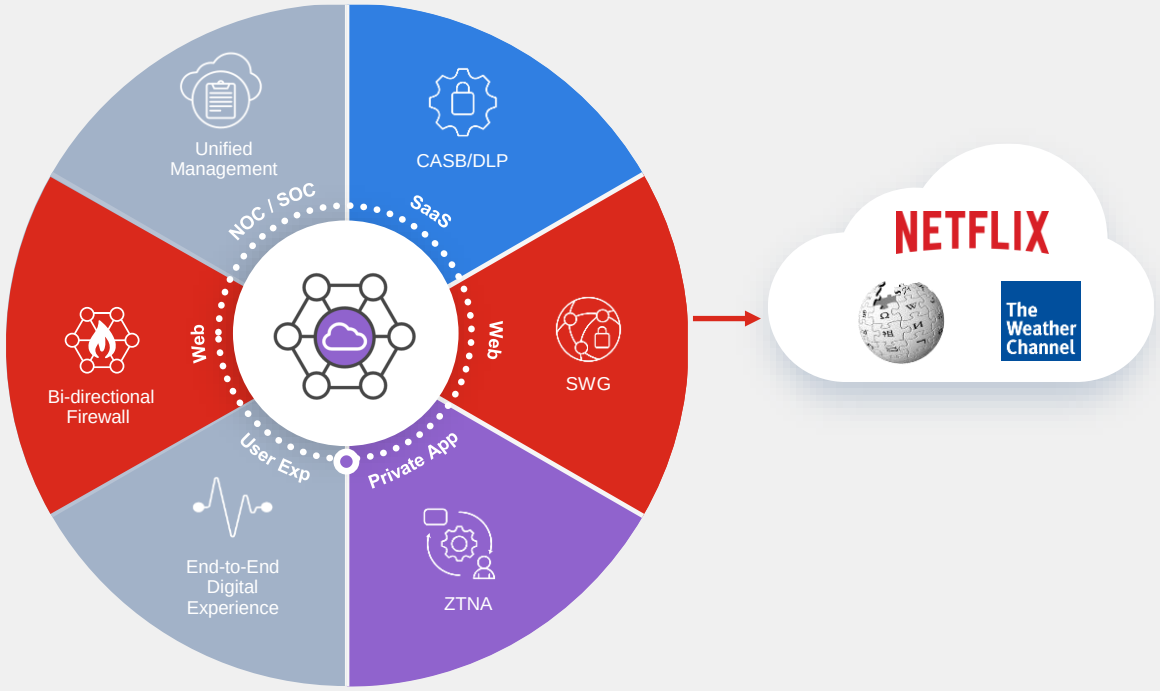
Для офісів та віддалених співробітників

Безпечний Інтернет

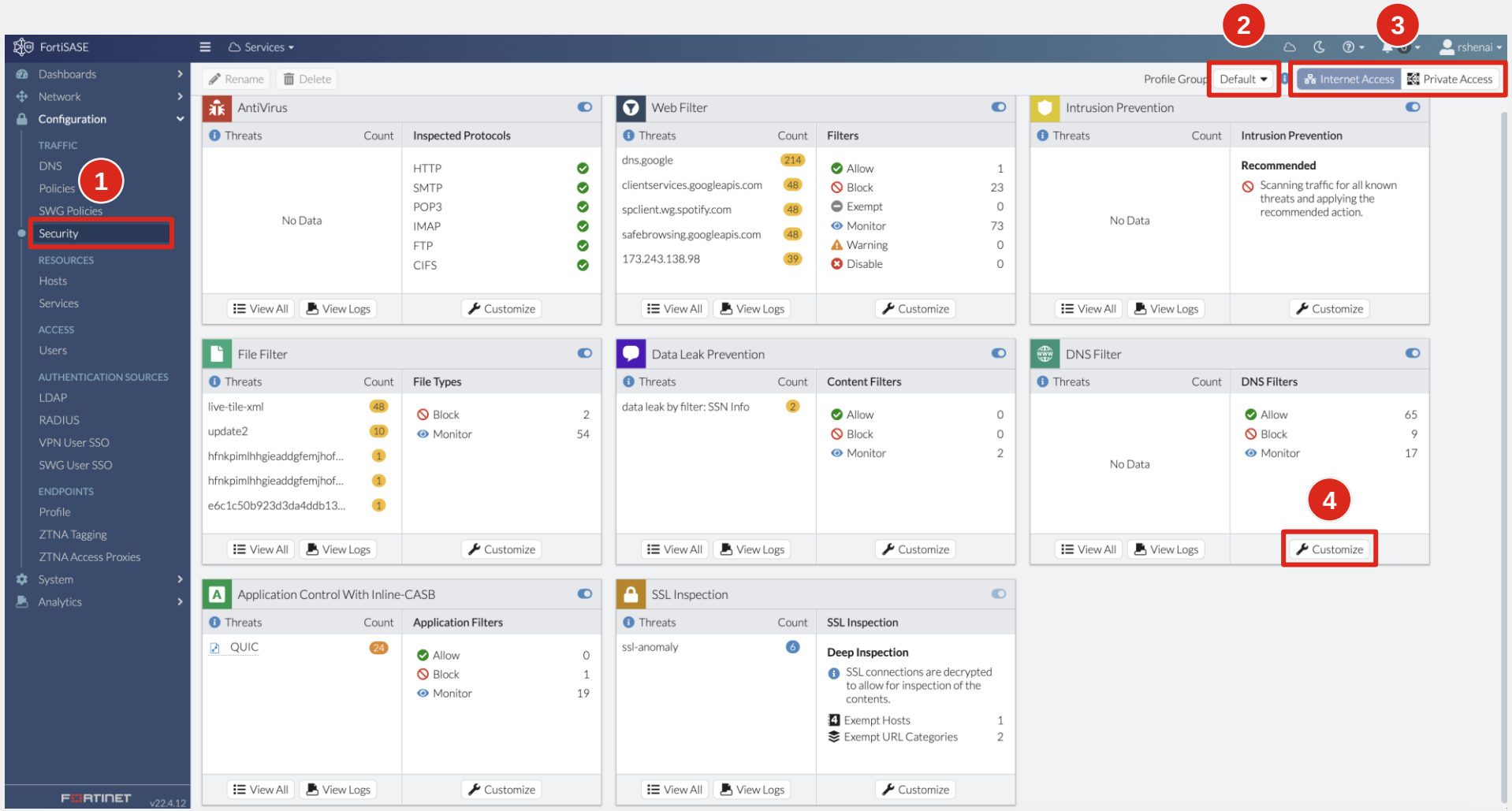
Захист від Malware & ransomware
Постійна оцінка вразливостей та протидія

Глибока перевірка трафіку
Постійна перевірка веб сайтів навіть коли використовується HTTPS

Перевірене рішення
FortiGuard Labs перевірений як тестами так і ринком



Безпечний Інтернет – Захист



1. Безпека з одного пункту
2. Готові профілі «з коробки»
3. Видимість публічних та приватних сервісів
4. Кастомізація безпеки

Безпечний доступ до SaaS

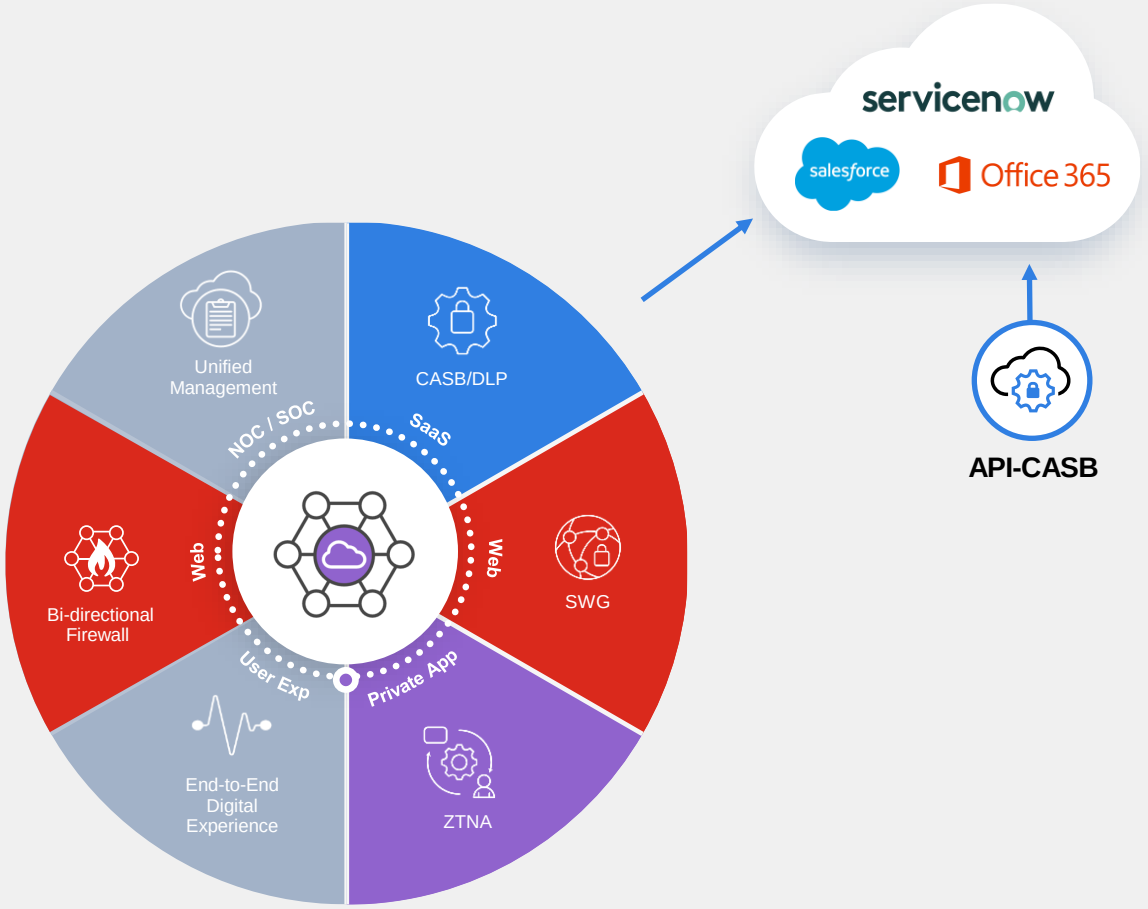
Видимість та контроль

Безпечний доступ до сервісів та файлів

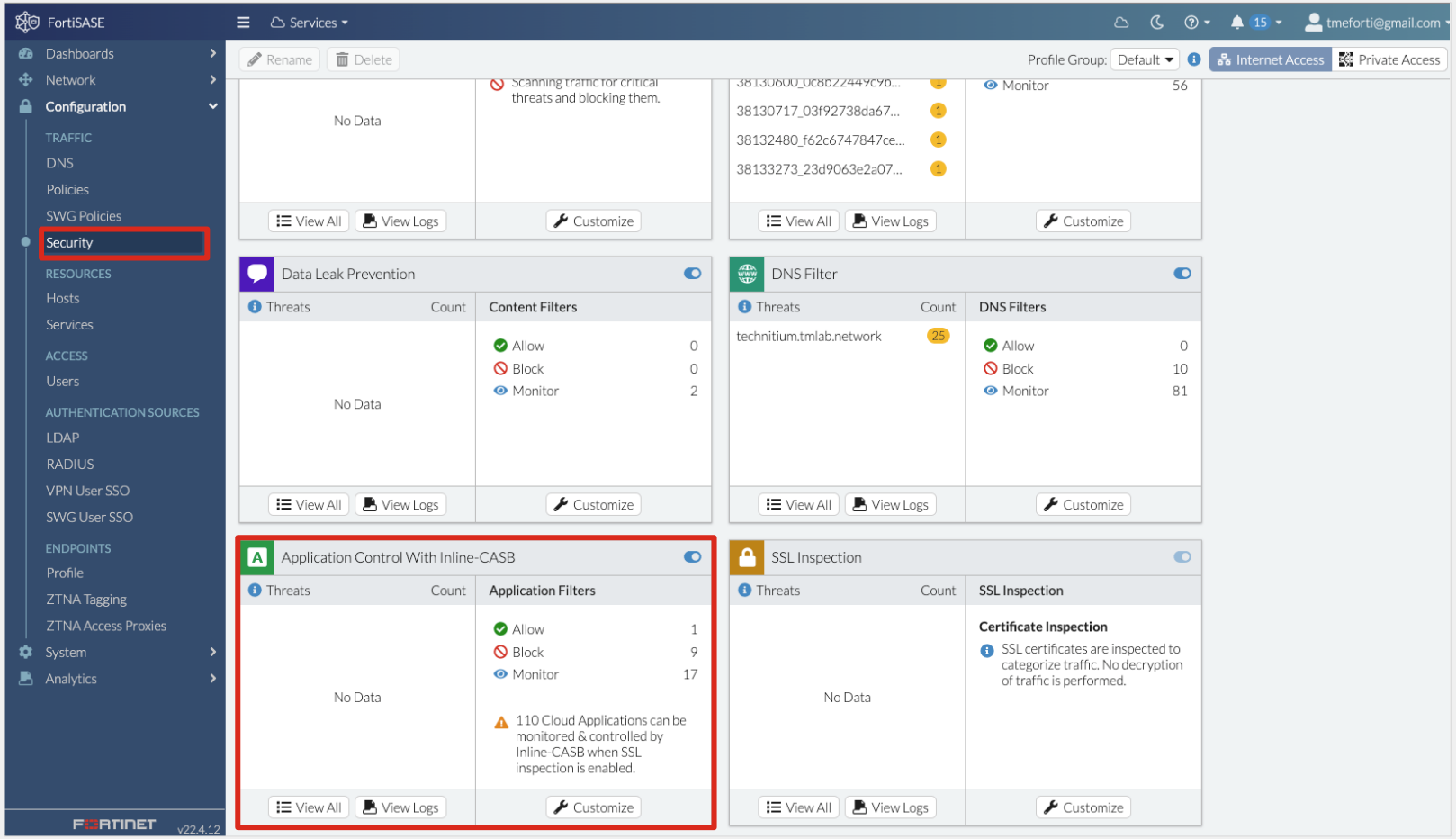
Контроль доступу до хмарних сервісів
Безпечний доступ до SaaS сервісів за допомогою CASB з використанням ZTNA

Контроль та перегляд вмісту
Контроль контенту та файлів з CASB API для деталізації безпеки

Уніфікований агент
FortiClient справляється як з SASE так і іншим (Zero-trust, SaaS безпека, захист ПК користувача)



Можливості CASB

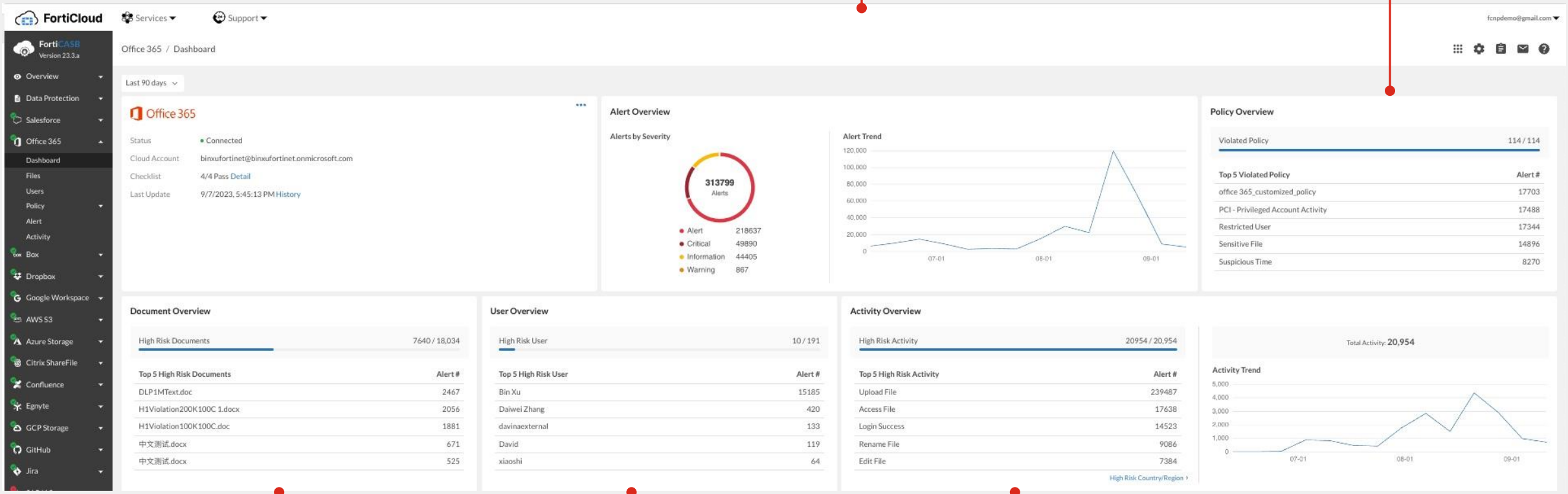


- Статус сервісу
- Історія активності
- Статистика ризиків
- Найризикованіші користувачі, файли, політики та країни
- Тренди ризиків та використання

Офіс 365 за останні 90 днів

Сповіщення & тренди

Спрацювання політик



Документи відмічені ризикованими

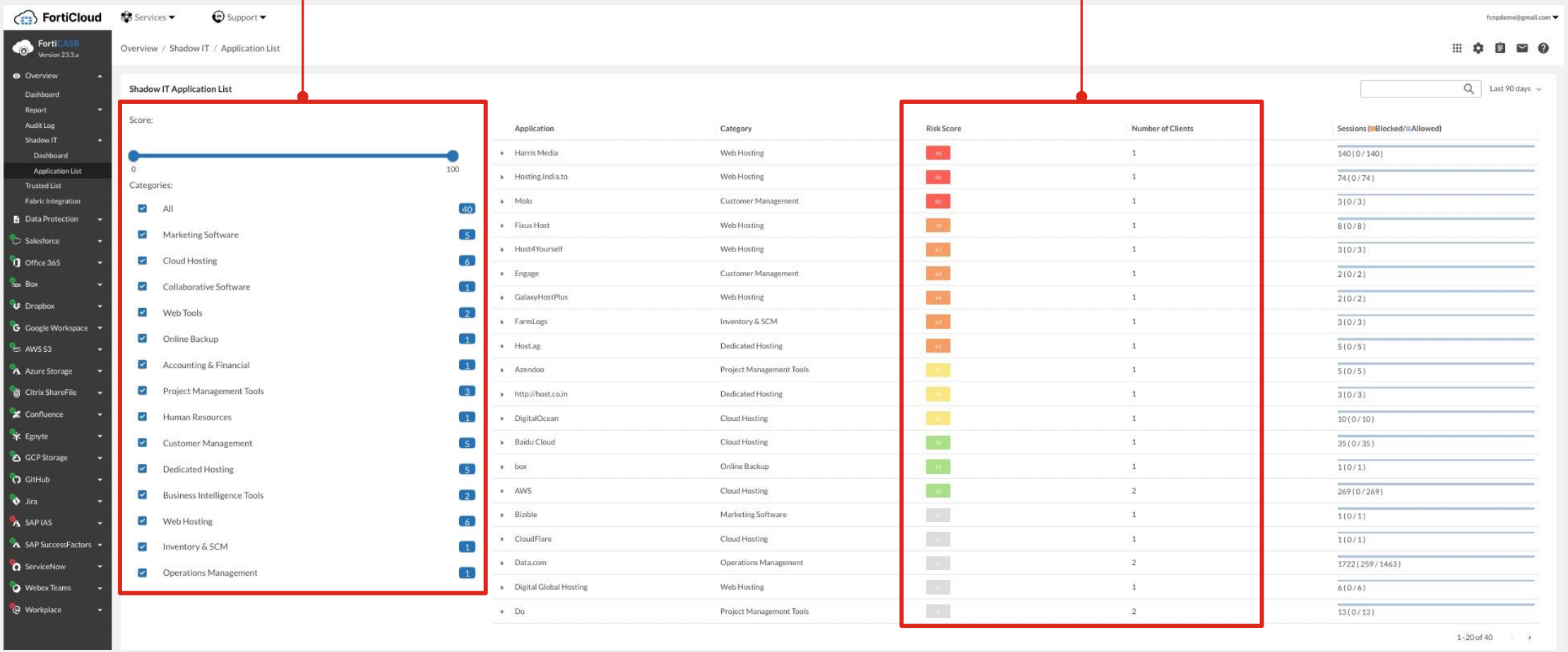
Користувачі відмічені ризикованими

Ризиковані **дії** користувачів

Наведення порядку парку ПЗ

Фільтр на основі ризиків або сервісу

Бали ризику



Гібридна інфраструктура. Наступний рівень.

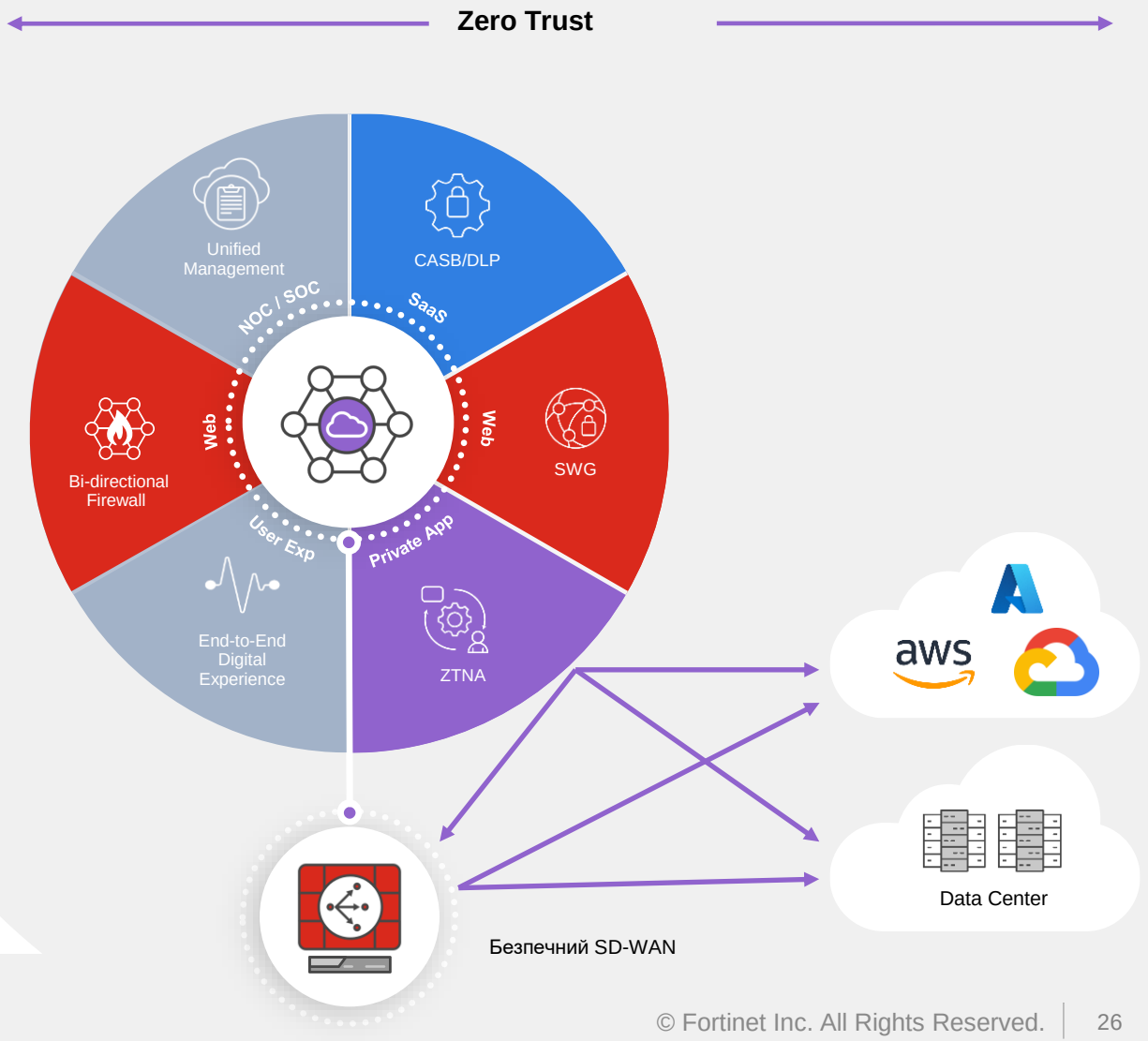
Разом з ZTNA та SD-WAN

Доступ до внутрішніх сервісів

Безпечний доступ в хмару/ЦОД
Захищений доступ до сервісів

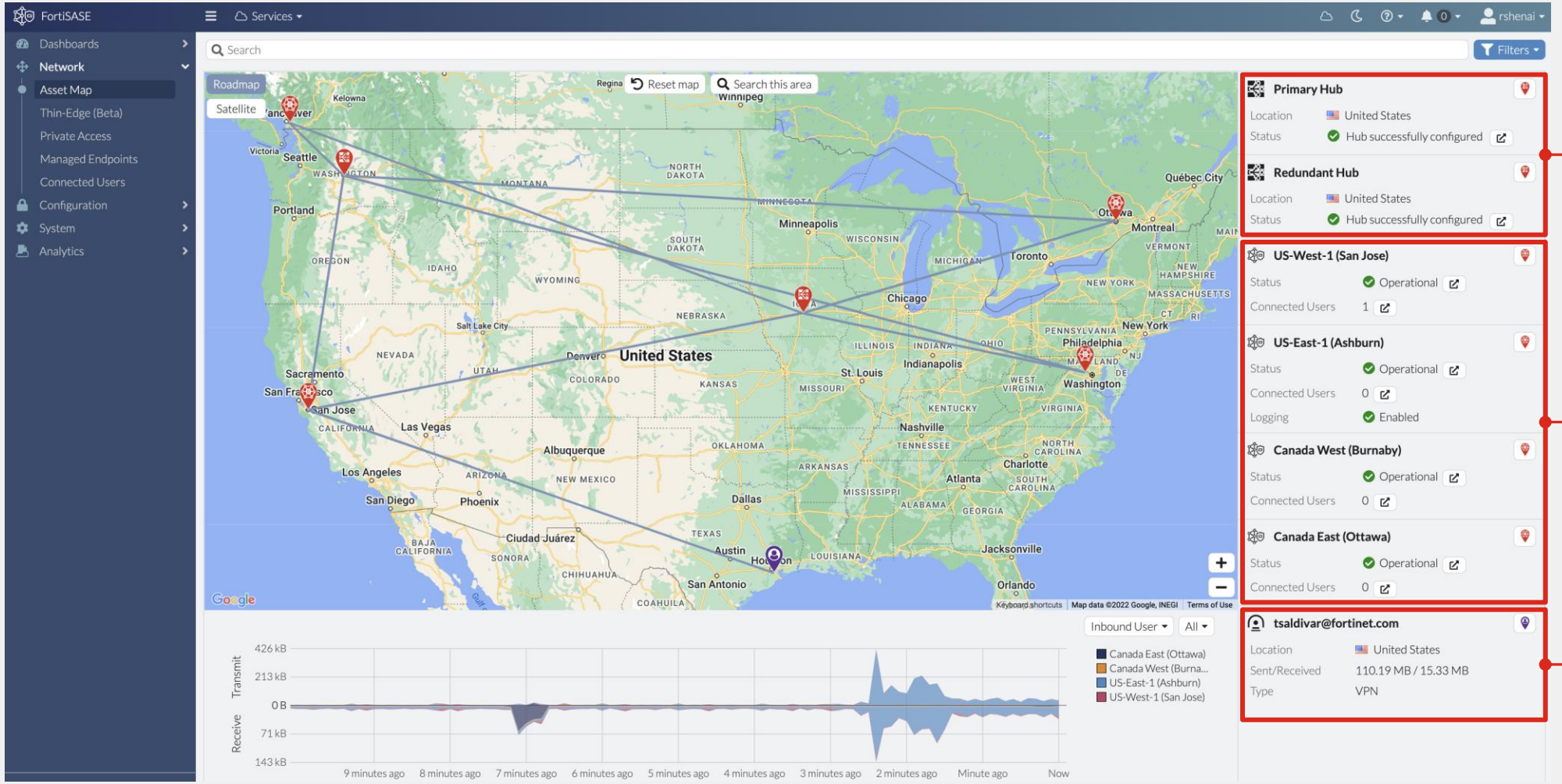
Детальний контроль доступу
Реалізація zero-trust на основі сервісів з використанням AI/ML

Інтеграція з існуючим SD-WAN
Відмінні відгуки користувачів за рахунок інтеграції з наявною Fortinet SD-WAN



FortiSASE SPA

Прозоре та безпечне підключення користувачів до їх сервісів



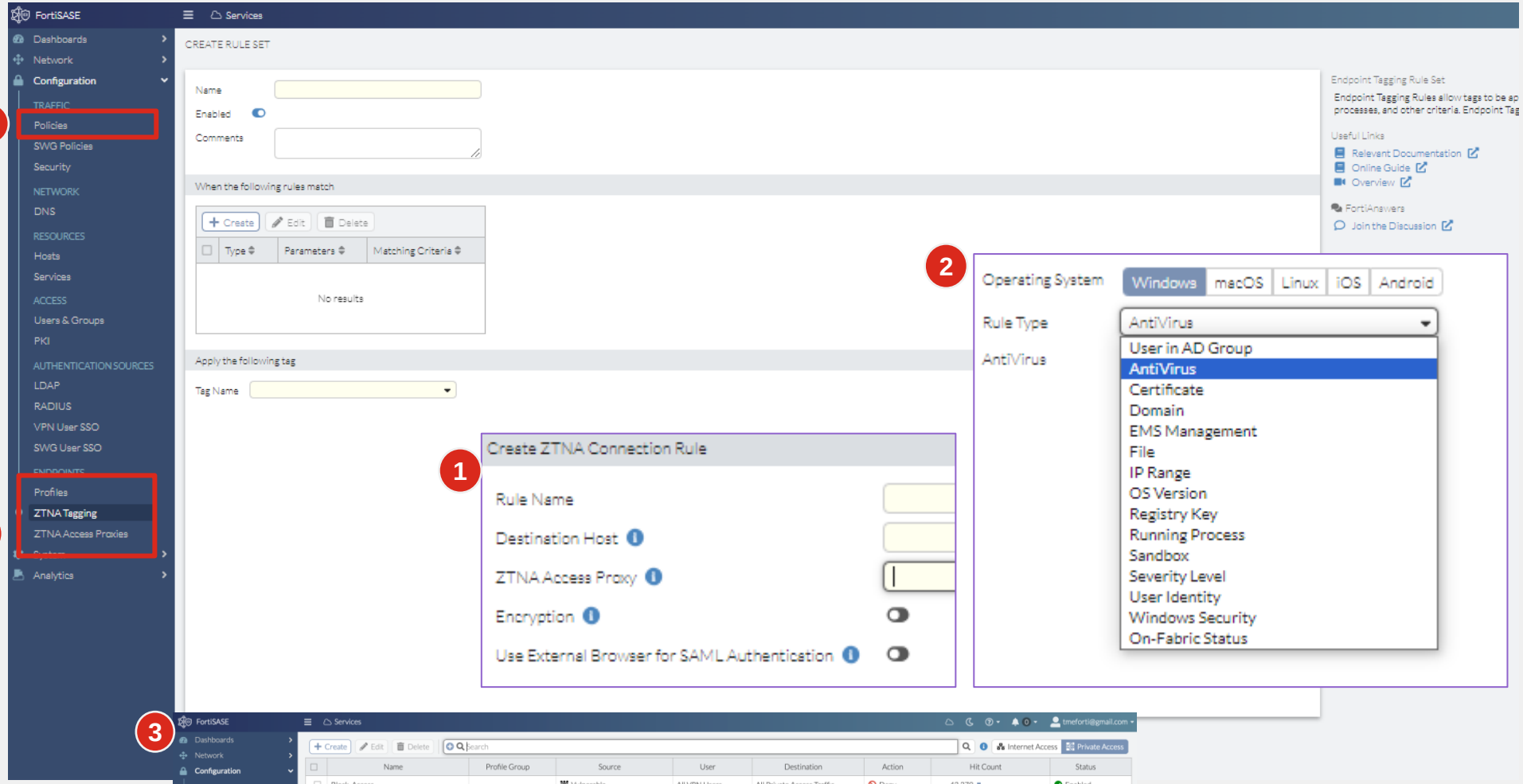
SD-WAN ЦОД

Доступні SASE точки (PoPs)

Користувачі

Zero Trust безпека для сервісів

Аутентифікація | Централізоване кеування | Постійні перевірки



1. ZTNA проксі
2. ZTNA теги
3. Політики на основі ZTNA тегів

Ліцензування

FortiSASE ліцензії

Capability	Standard Subscription	Advanced Subscription
SWG	●	●
FWaaS	●	●
FortiClient & EPP	●	●
ZTNA	●	●
CASB (Inline and API)	●	●
Data Loss Prevention (DLP)	●	●
Sandbox	●	●
Digital Experience Monitoring (DEM)		●
SOCaaS Integration		●
Endpoint Forensics		●
Dedicated IPs	*Add-on*	●
Assisted On-boarding		●

Обмеження

3 пристрої для кожного користувача
4 ЦОД в комплекті (можна розширити)
FortiCare Premiun 24/7 в комплекті
Для підключення FortiGate потрібна додаткова ліцензія

FortiSASE ліцензії

	REMOTE USERS		
	STANDARD	ADVANCED	COMPREHENSIVE
Secure Internet Access (SIA)			
SSL Inspection	✓	✓	✓
Inline Anti-virus (AV) and Sandbox	✓	✓	✓
Intrusion Prevention	✓	✓	✓
Web and DNS Filtering	✓	✓	✓
Botnet C&C Filtering	✓	✓	✓
Secure SaaS Access (SSA)			
Inline CASB	✓	✓	✓
Inline DLP	✓	✓	✓
Cloud API CASB & DLP	License Included	License Included	License Included
Secure Private Access (SPA)			
FortiGate Private Access	✓ ①	✓ ①	✓ ①
Zero Trust Network Access (ZTNA)	✓	✓	✓
License Includes			
Devices per User	Up to 3 ②	Up to 3 ②	Up to 3 ②
Dedicated Public IPs	Add-on	✓	✓
Endpoint Security ③			
Vulnerability Management	✓	✓	✓
Endpoint Protection Platform	✓	✓	✓
OS Support	Windows, MacOS, Linux, iOS, Android	Windows, MacOS, Linux, iOS, Android	Windows, MacOS, Linux, iOS, Android
NOC / SOC Integration			
SASE Cloud Management	✓	✓	✓
REST API	✓	✓	✓
[illegible]			✓
Digital Experience Monitoring		✓ ③	✓ ③
SOC-as-a-Service Integration		✓	✓
FortiGuard Forensics (Response) Service		✓ ③	✓ ③
[illegible]			
Locations	Fortinet Cloud Locations	Fortinet Cloud Locations	Public Cloud Locations
Customer Support Services			
24×7 Premium Support	✓	✓	✓
Assisted On-boarding		✓	✓

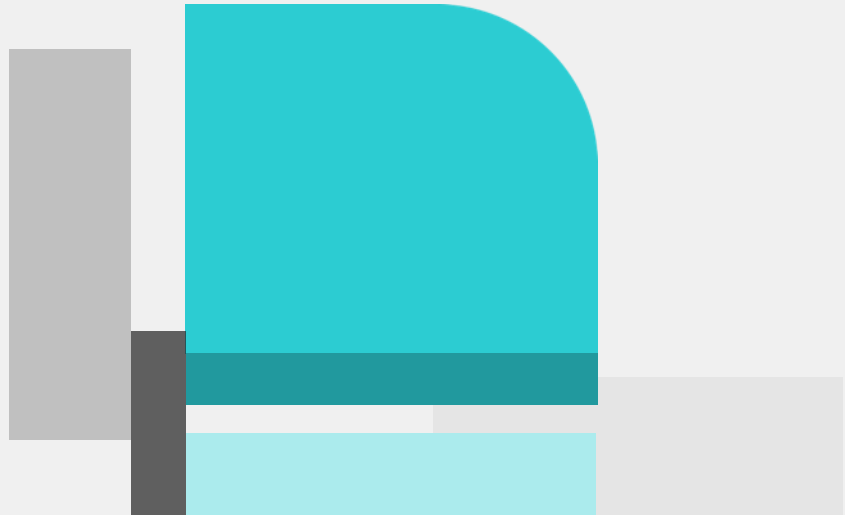
Доп. опції

OPTION	QUANTITY
Bandwidth Add-on	25 Mbps
Dedicated Public IP Address	4 x Public IP Addresses
FortiGate SPA	License required per FortiGate
Fortinet Location Add-on	1 Location
Public Cloud Location Add-on	1 Location

Наявні FortiGate

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS Service	•	•	•	•
	Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	URL, DNS & Video Filtering Service	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention Service	•	•		
	Data Loss Prevention Service [1]	•	•		
	OT Security Service (OT Detection, OT Vulnerability correlation, Virtual Patching, OT Signature / Protocol Decoders) [1]	•			
	Application Control		included with FortiCare Subscription		
	CASB SaaS Control		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
	SD-WAN Overlay-as-a-Service for SaaS-based overlay network provisioning	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	FortiSASE subscription including cloud management and 10Mbps bandwidth license [2]	•			
NOC and SOC Services	FortiGuard Attack Surface Security Service (IoT Detection, IoT Vulnerability Correlation, and Security Rating Updates) [1]	•	•		
	FortiConverter Service	•	•		
	Managed FortiGate Service	•			
	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiManager Cloud	•			
	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
	FortiGuard SOCaaS	•			
Hardware and Software Support	FortiCare Essentials [2]	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Internet Service (SaaS) DB Updates	included with FortiCare Subscription			
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

Як виглядає?



Старт

https://support.fortinet.com/asset/#/dashboard

FortiCloud | Services | Support | ytaran@fortinet.com

ASSET MANAGEMENT

- Dashboard
- Products
- Marketplace
- Account Services

ASSETS & ACCOUNTS

- Asset Management
- IAM
- FortiFlex

CLOUD MANAGEMENT

- FortiClient EMS Cloud
- FortiGate Cloud
- FortiAnalyzer Cloud
- FortiManager Cloud
- FortiLAN Cloud

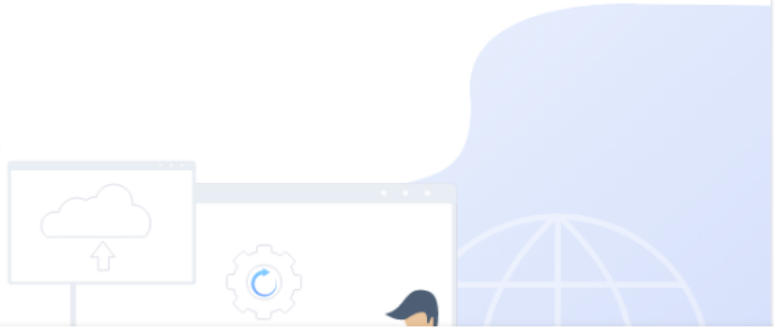
CLOUD SERVICES

- FortiSASE
- FortiMonitor
- FortiRecon
- FortiConverter
- FortiMail
- SOCaaS
- FortiWeb Cloud
- FortiZTP (Beta)

Show More

Registering more Fortinet products with Asset Management

You must register your products to receive FortiGuard



Corporate How to Buy Products Services & Support Legal Privacy Terms of Use

Старт

https://portal.prod.fortisase.com

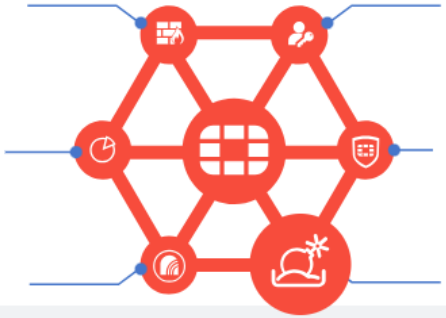
FortiSASE | Services | Support | ytaran@fortinet.com

Welcome to FortiSASE

Cloud-based policy enforcement powered by FortiOS

Advanced analytics powered by FortiAnalyzer

Zero-Trust Network Access



SSO-integration via SAML for VPN and SWG

Endpoint management powered by EMS and FortiClient

Built-in FortiSandbox

Entitlements

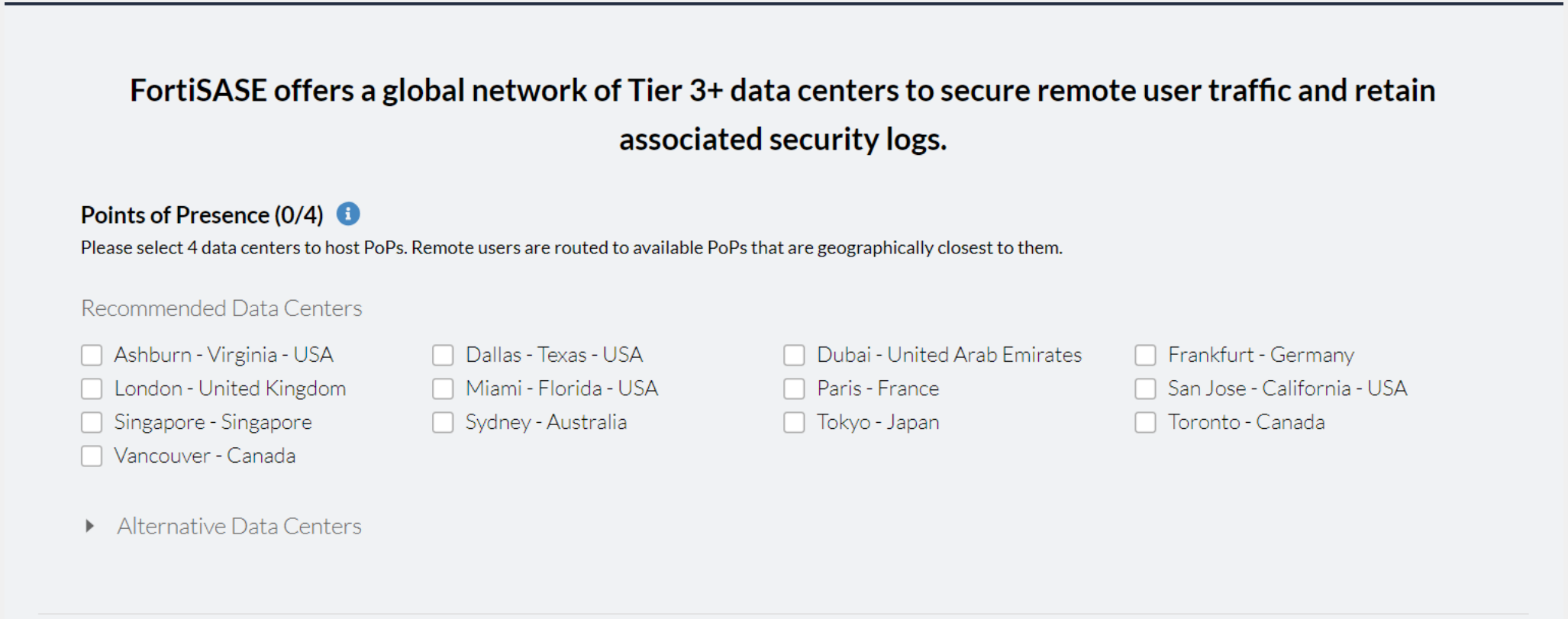
Endpoint Protection & Cloud Sandbox: 0

FortiSASE User Based Agents: 50

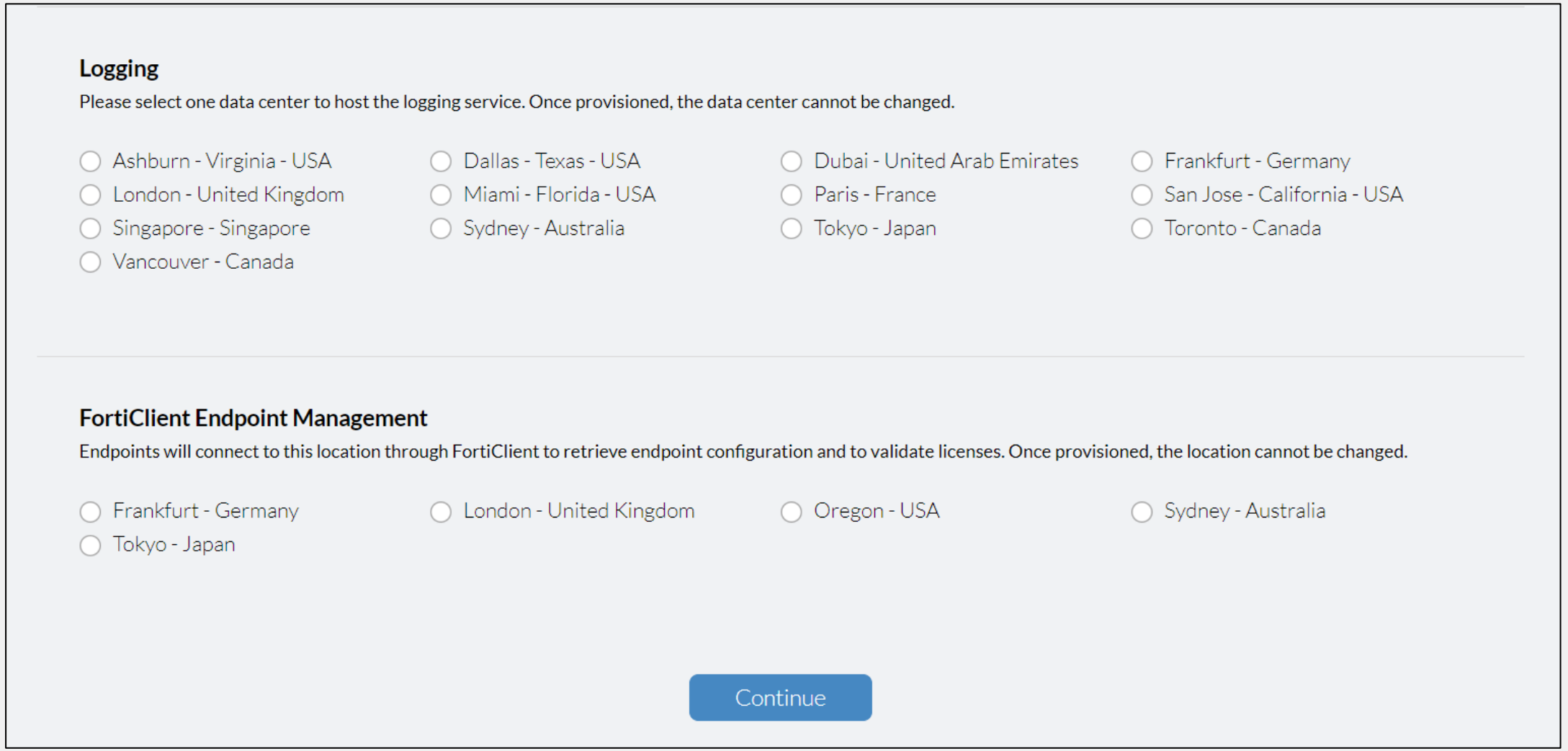
You will need to select data centers close to your end-users during provisioning.
Provisioning generally takes **around 10 minutes** but FortiSASE saves your provision progress if you are interrupted.

Start Onboarding

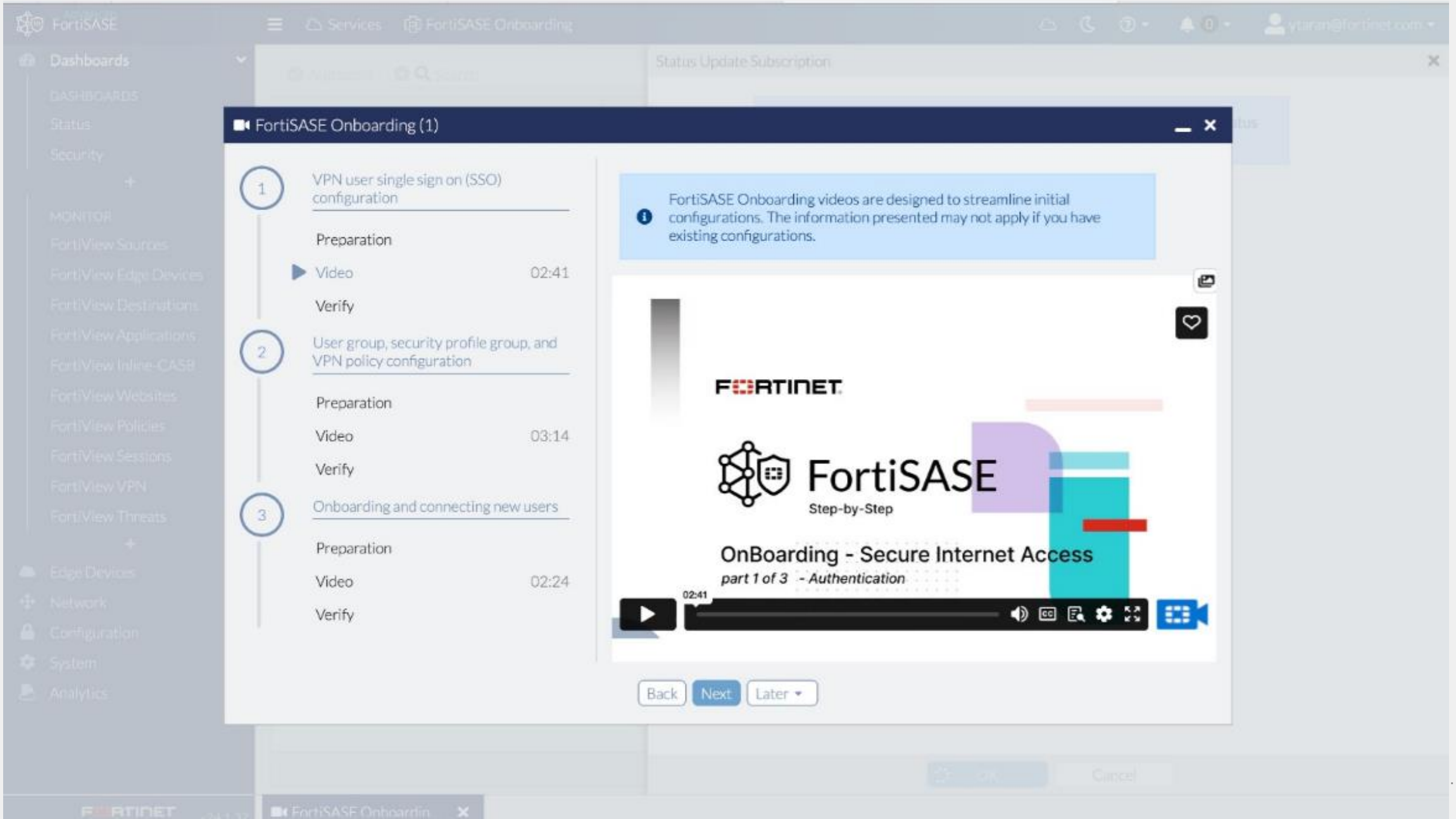
Старт



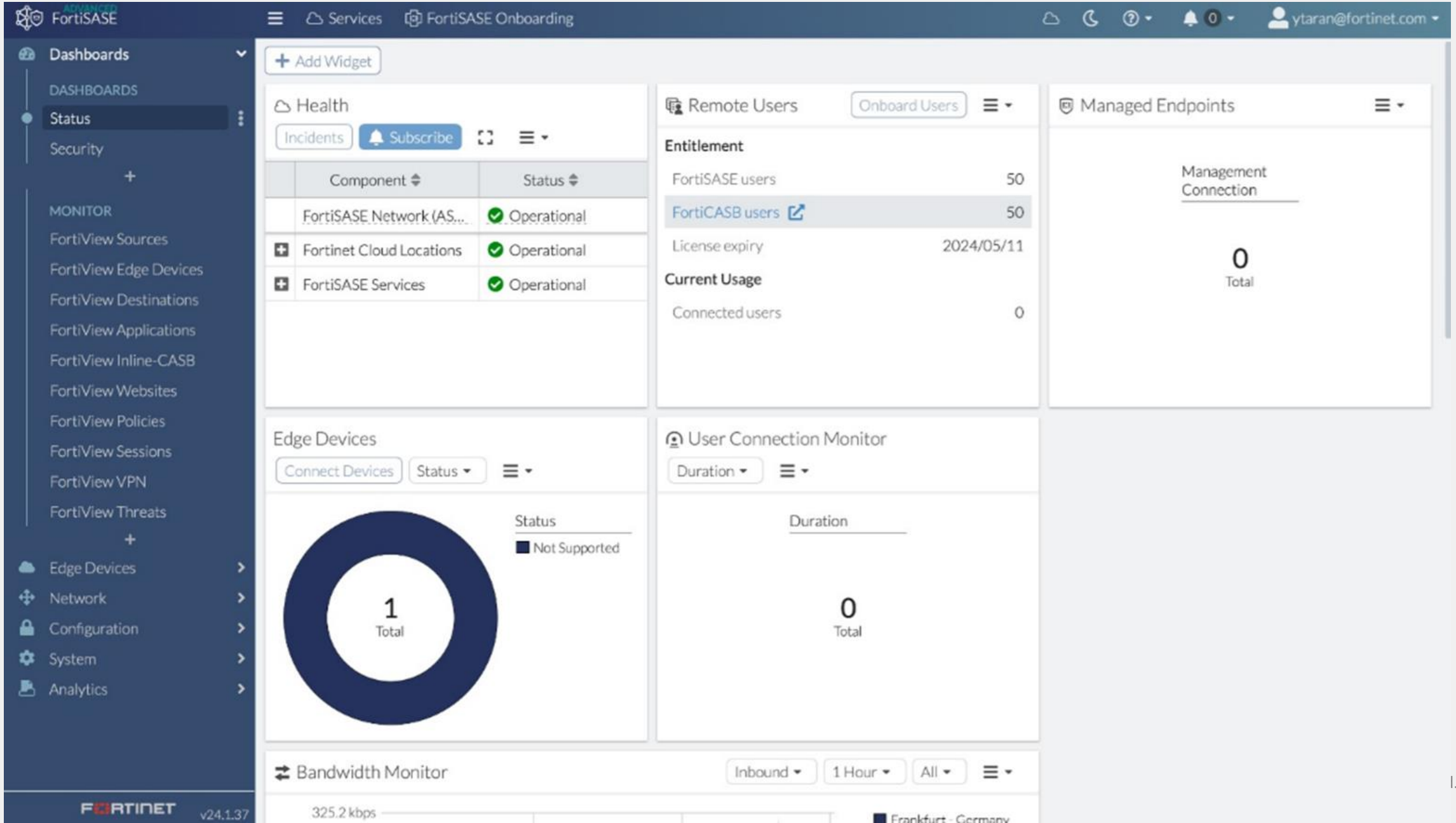
Старт



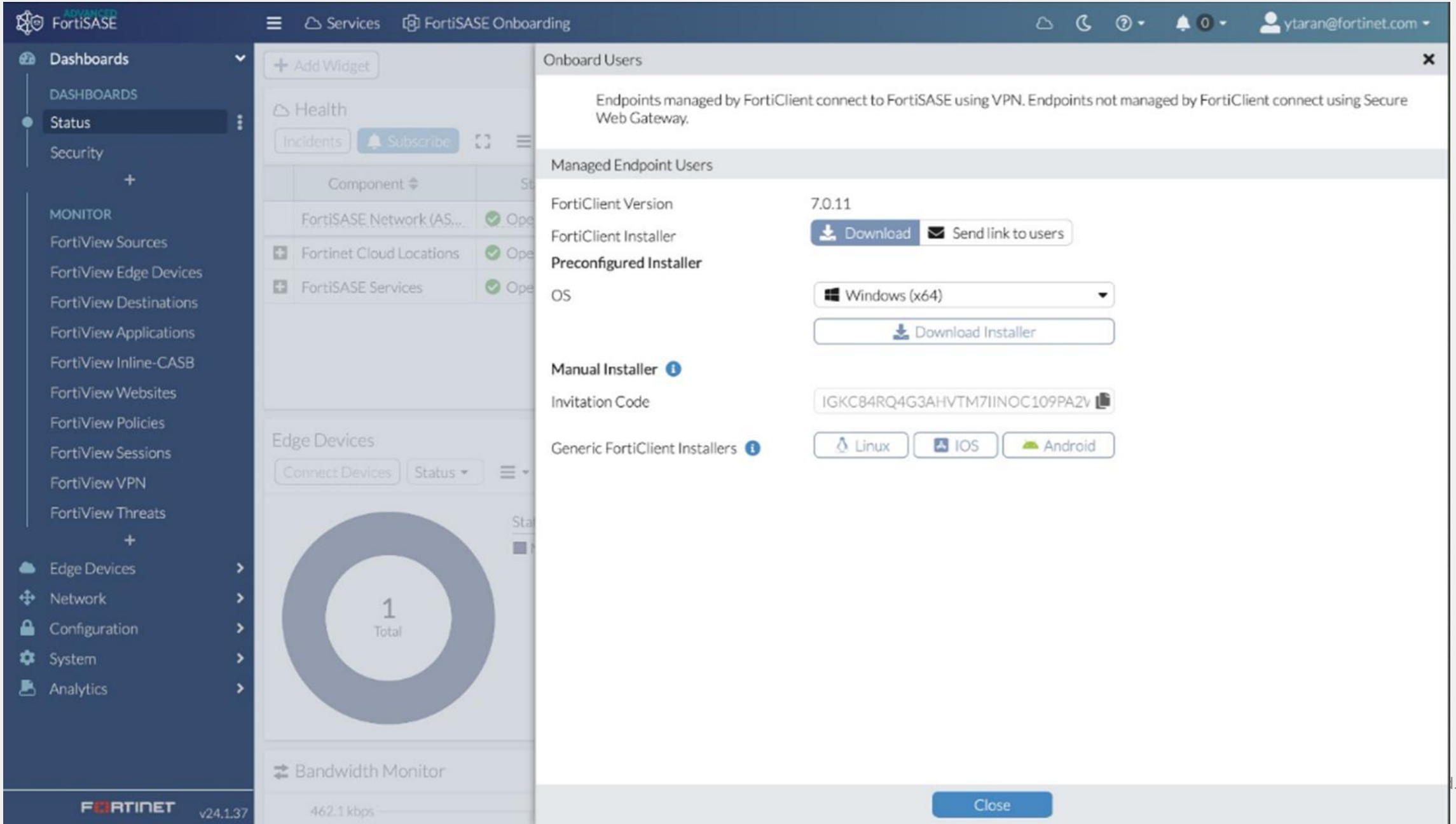
Стартове навчання



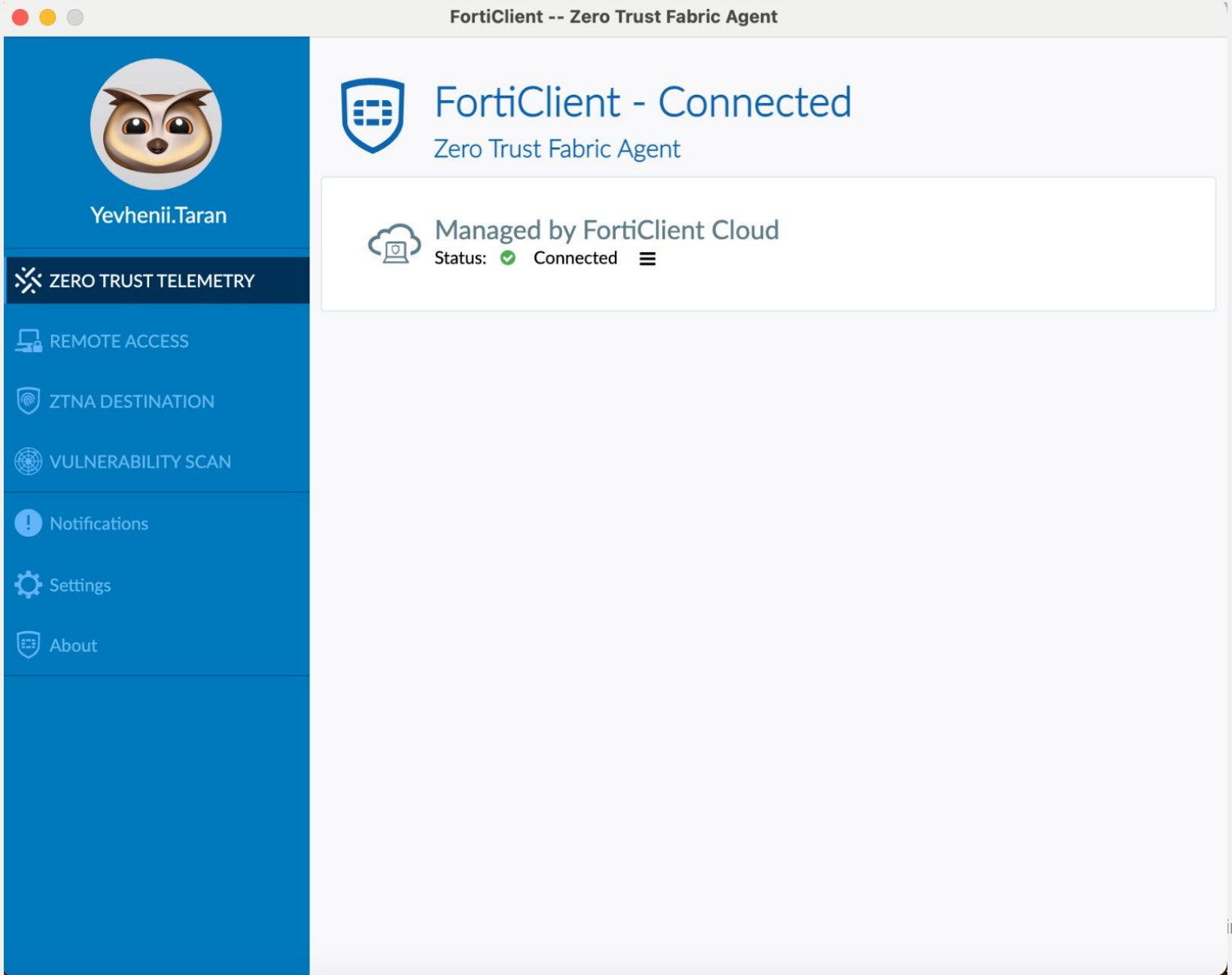
Перші кроки


FortiSASE
Services
FortiSASE Onboarding
ytaran@fortinet.com
Dashboards
DASHBOARDS
Status
Security
MONITOR
FortiView Sources
FortiView Edge Devices
FortiView Destinations
FortiView Applications
FortiView Inline-CASB
FortiView Websites
FortiView Policies
FortiView Sessions
FortiView VPN
FortiView Threats
Edge Devices
Network
Configuration
System
Analytics
FORTINET
v24.1.37
Add Widget
Health
Incidents
Subscribe
Component
Status
FortiSASE Network (AS...
Operational
Fortinet Cloud Locations
Operational
FortiSASE Services
Operational
Remote Users
Onboard Users
Entitlement
FortiSASE users
50
FortiCASB users
50
License expiry
2024/05/11
Current Usage
Connected users
0
Managed Endpoints
Management Connection
0
Total
Edge Devices
Connect Devices
Status
Status
Not Supported
1
Total
User Connection Monitor
Duration
Duration
0
Total
Bandwidth Monitor
Inbound
1 Hour
All
325.2 kbps
Frankfurt - Germany

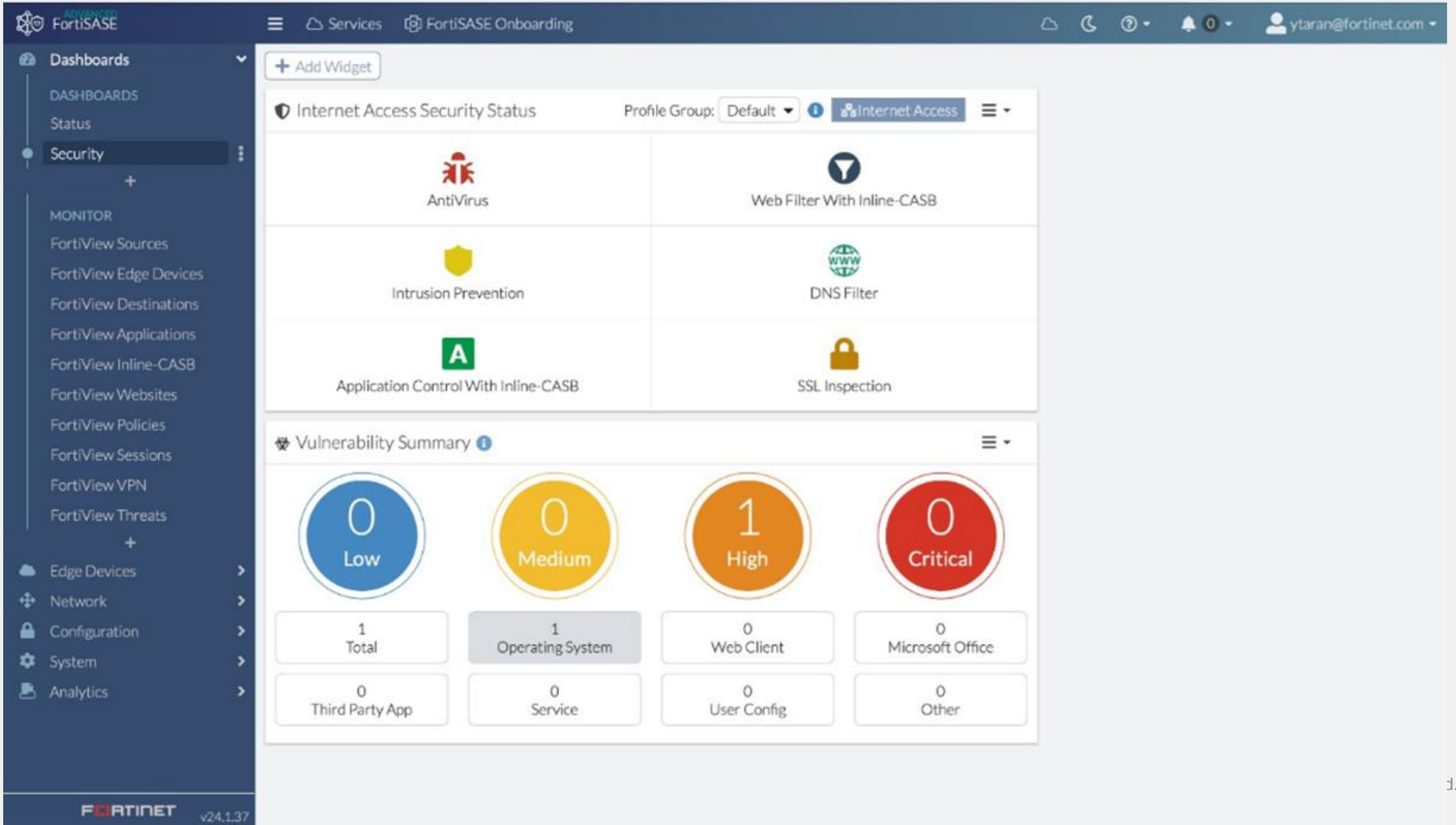
Перші кроки


FortiSASE
Services
FortiSASE Onboarding
ytaran@fortinet.com
Dashboards
DASHBOARDS
Status
Security
MONITOR
FortiView Sources
FortiView Edge Devices
FortiView Destinations
FortiView Applications
FortiView Inline-CASB
FortiView Websites
FortiView Policies
FortiView Sessions
FortiView VPN
FortiView Threats
Edge Devices
Network
Configuration
System
Analytics
FORTINET
v24.1.37
Add Widget
Health
Incidents
Subscribe
Component
FortiSASE Network (AS...
Fortinet Cloud Locations
FortiSASE Services
Edge Devices
Connect Devices
Status
1
Total
Bandwidth Monitor
462.1 kbps
Onboard Users
Endpoints managed by FortiClient connect to FortiSASE using VPN. Endpoints not managed by FortiClient connect using Secure Web Gateway.
Managed Endpoint Users
FortiClient Version
7.0.11
FortiClient Installer
Download
Send link to users
Preconfigured Installer
OS
Windows (x64)
Download Installer
Manual Installer
Invitation Code
IGKC84RQ4G3AHVTM7IINOC109PA2V
Generic FortiClient Installers
Linux
IOS
Android
Close

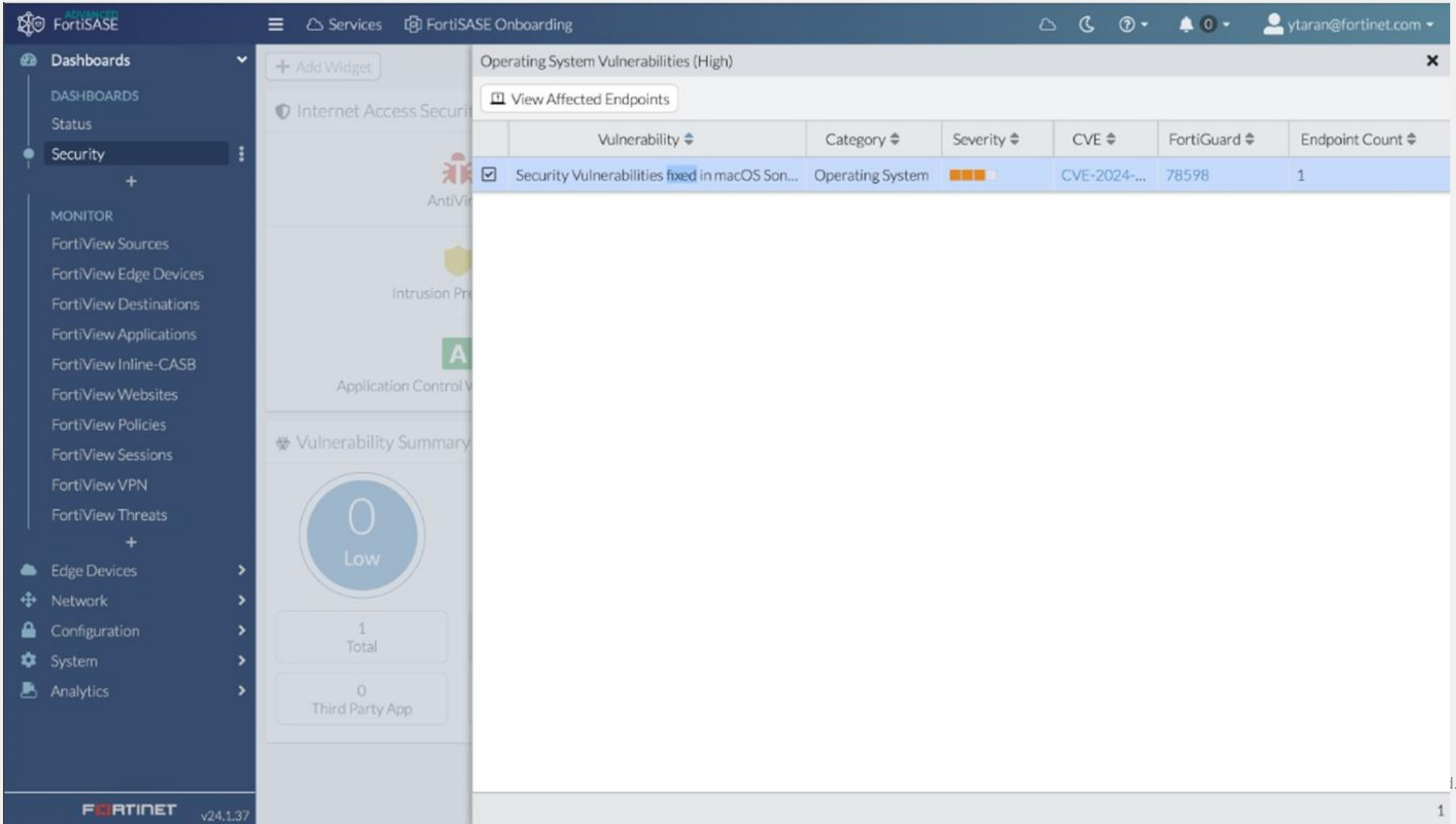
Перші кроки



Перші кроки

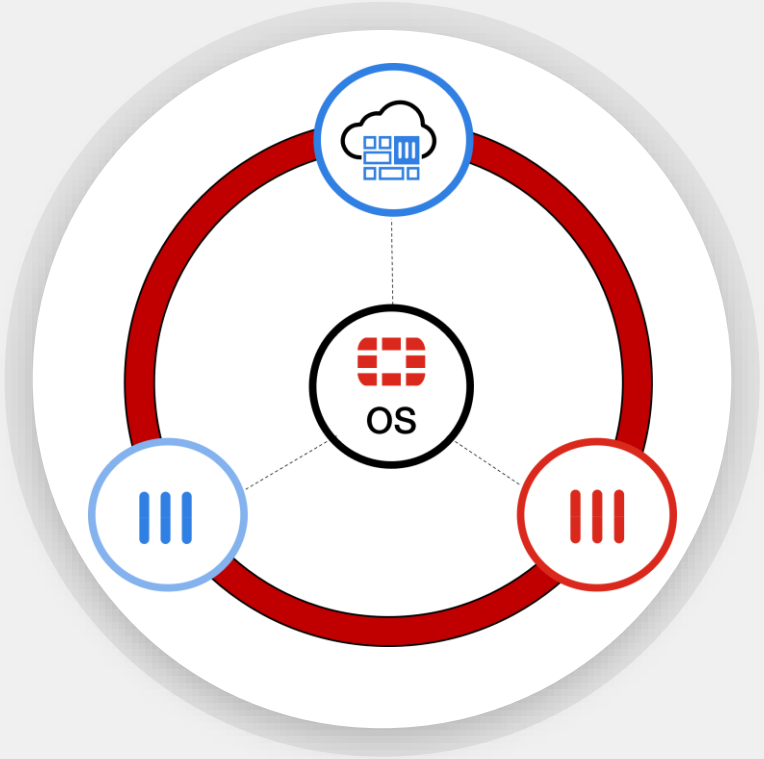

FortiSASE
Services
FortiSASE Onboarding
ytaran@fortinet.com
Dashboards
DASHBOARDS
Status
Security
MONITOR
FortiView Sources
FortiView Edge Devices
FortiView Destinations
FortiView Applications
FortiView Inline-CASB
FortiView Websites
FortiView Policies
FortiView Sessions
FortiView VPN
FortiView Threats
Edge Devices
Network
Configuration
System
Analytics
FORTINET
v24.1.37
Add Widget
Internet Access Security Status
Profile Group: Default
Internet Access
AntiVirus
Web Filter With Inline-CASB
Intrusion Prevention
DNS Filter
Application Control With Inline-CASB
SSL Inspection
Vulnerability Summary
0 Low
0 Medium
1 High
0 Critical
1 Total
1 Operating System
0 Web Client
0 Microsoft Office
0 Third Party App
0 Service
0 User Config
0 Other

Перші кроки

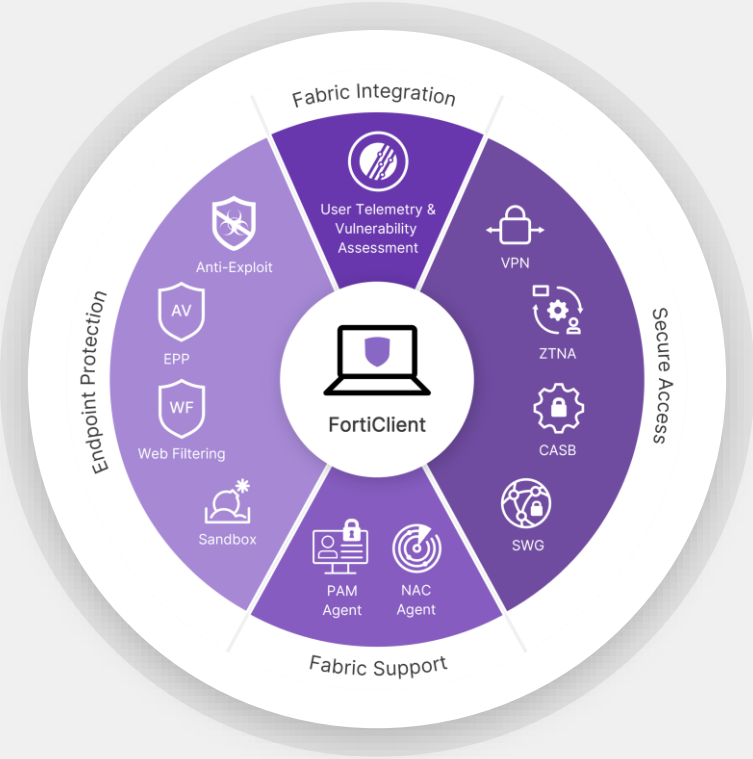

FortiSASE
Services
FortiSASE Onboarding
ytaran@fortinet.com
Dashboards
DASHBOARDS
Status
Security
MONITOR
FortiView Sources
FortiView Edge Devices
FortiView Destinations
FortiView Applications
FortiView Inline-CASB
FortiView Websites
FortiView Policies
FortiView Sessions
FortiView VPN
FortiView Threats
Edge Devices
Network
Configuration
System
Analytics
FORTINET
v24.1.37
Add Widget
Internet Access Securit
Intrusion Pre
Application Control V
Vulnerability Summary
0
Low
1
Total
0
Third Party App
Operating System Vulnerabilities (High)
View Affected Endpoints
Vulnerability
Category
Severity
CVE
FortiGuard
Endpoint Count
Security Vulnerabilities fixed in macOS Son...
Operating System
CVE-2024-...
78598
1
1

Висновки

FortiSASE



Працює як єдиний організм

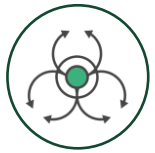


Уніфікований агент

Перевірені AI сервіси та сигнатури

Ключове

Комплексний захист

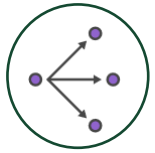


Використання AI механізмів
Безпека від Ransomware
Безпечний Інтернет

Міграція з VPN до ZTNA

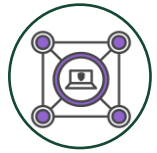
Оркестрація доступу
Постійний моніторинг відповідності
Моніторинг загроз

Оптимізація швидкодії



Модернізація мережі
Контроль досвіду користувача
Прискорення трафіку

Спрощення керування та звітності



Видимість користувачів, ПЗ та безпеки
Консолідація мережі та безпеки
Одна консоль та один агент

Інвентаризація пристроїв та ПЗ

Моніторинг сервісів
Оцінка ризиків
Політики

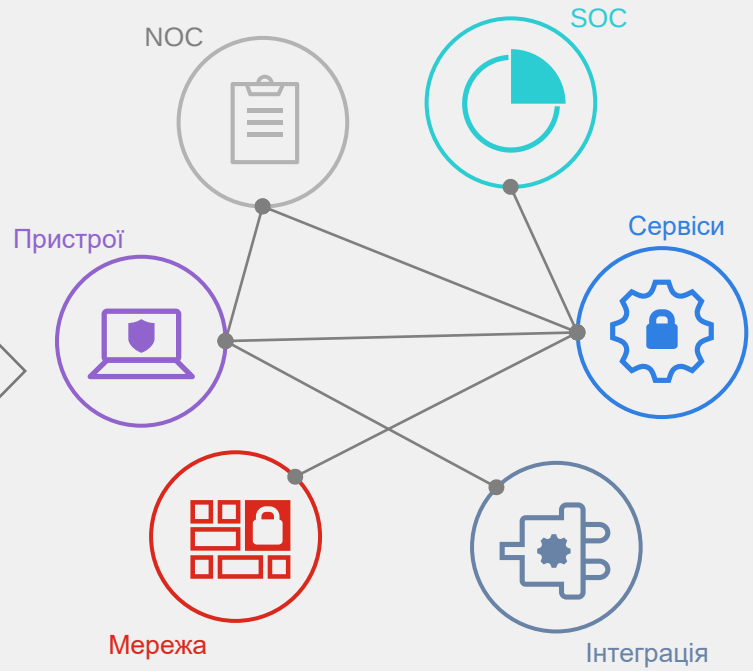
Конфіденційність даних та compliance

Захист критичних даних
Виконання вимог регуляторів
Захист персональної інформації

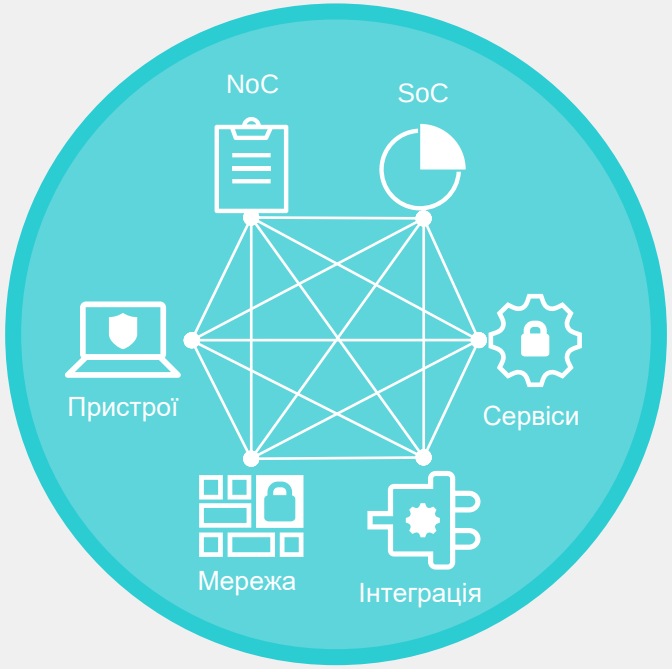
Fortinet – еволюція IT

30+ виробників

10 виробників



2-3 платформи



Еволюція

Дякую за увагу!