



FortiSASE. Побудова IT інфраструктури та безпеки сервісів без датацентрів

Євгеній Таран, Systems Engineer

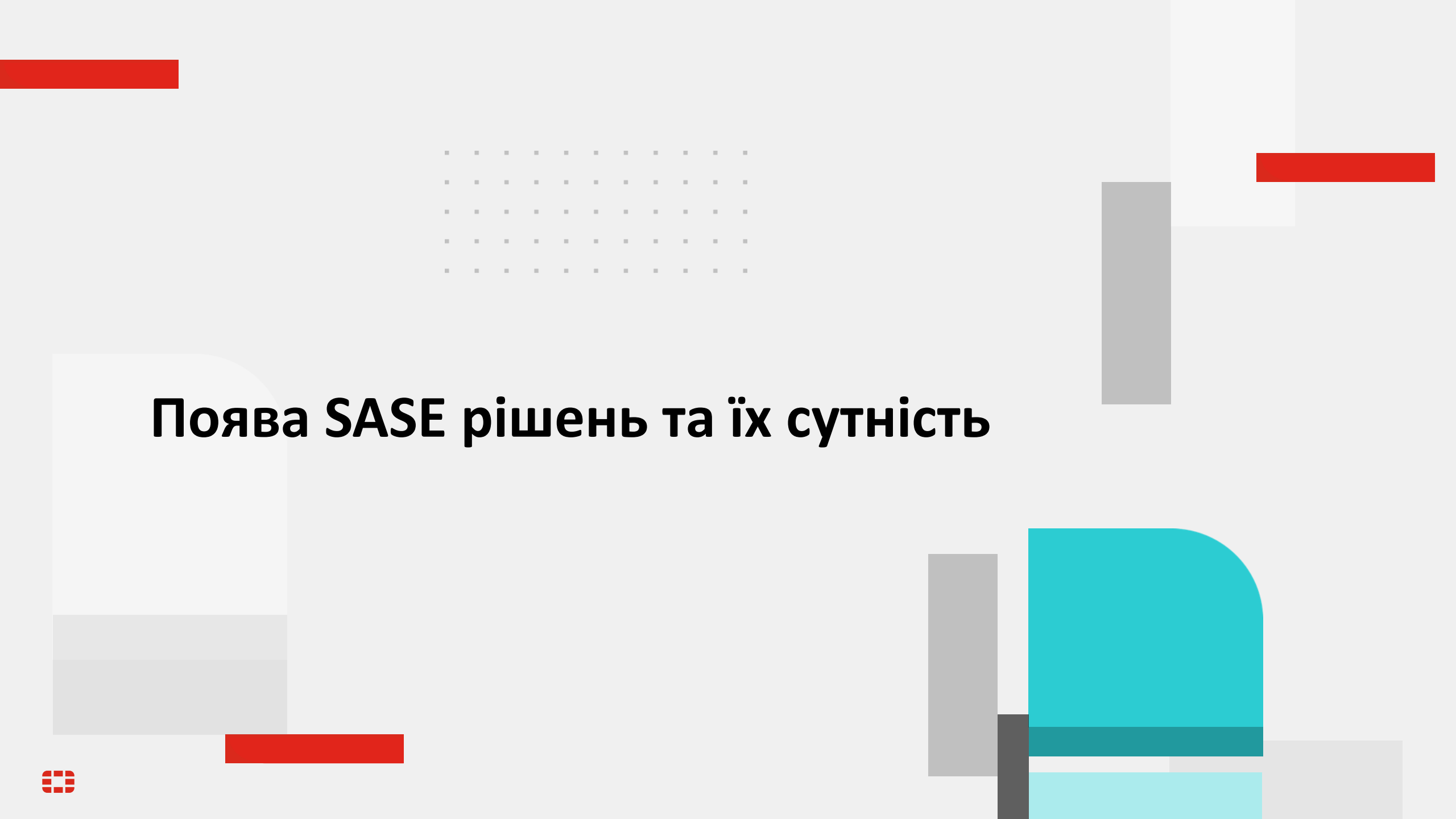
ytaran@fortinet.com

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

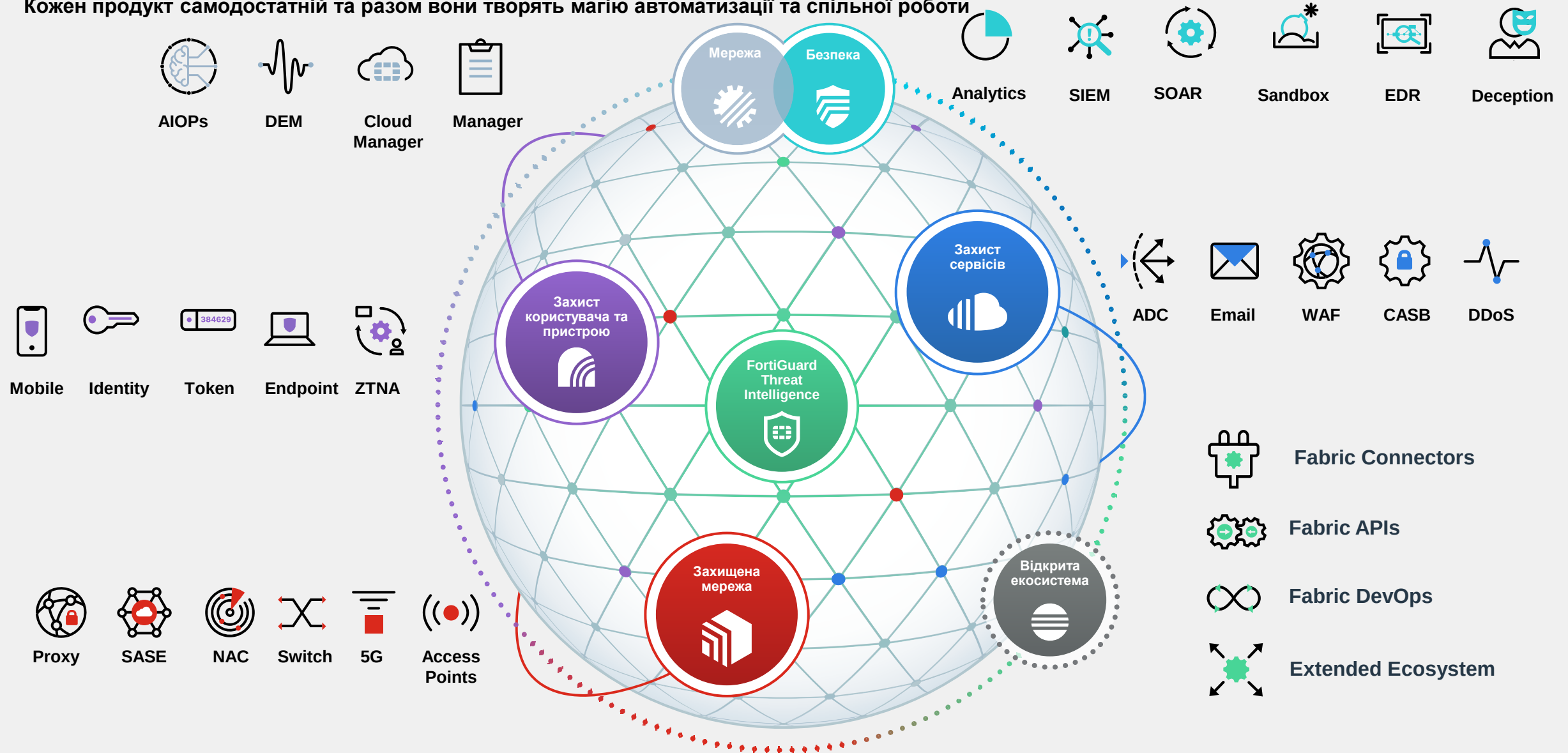


Сучасні реалії

- 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

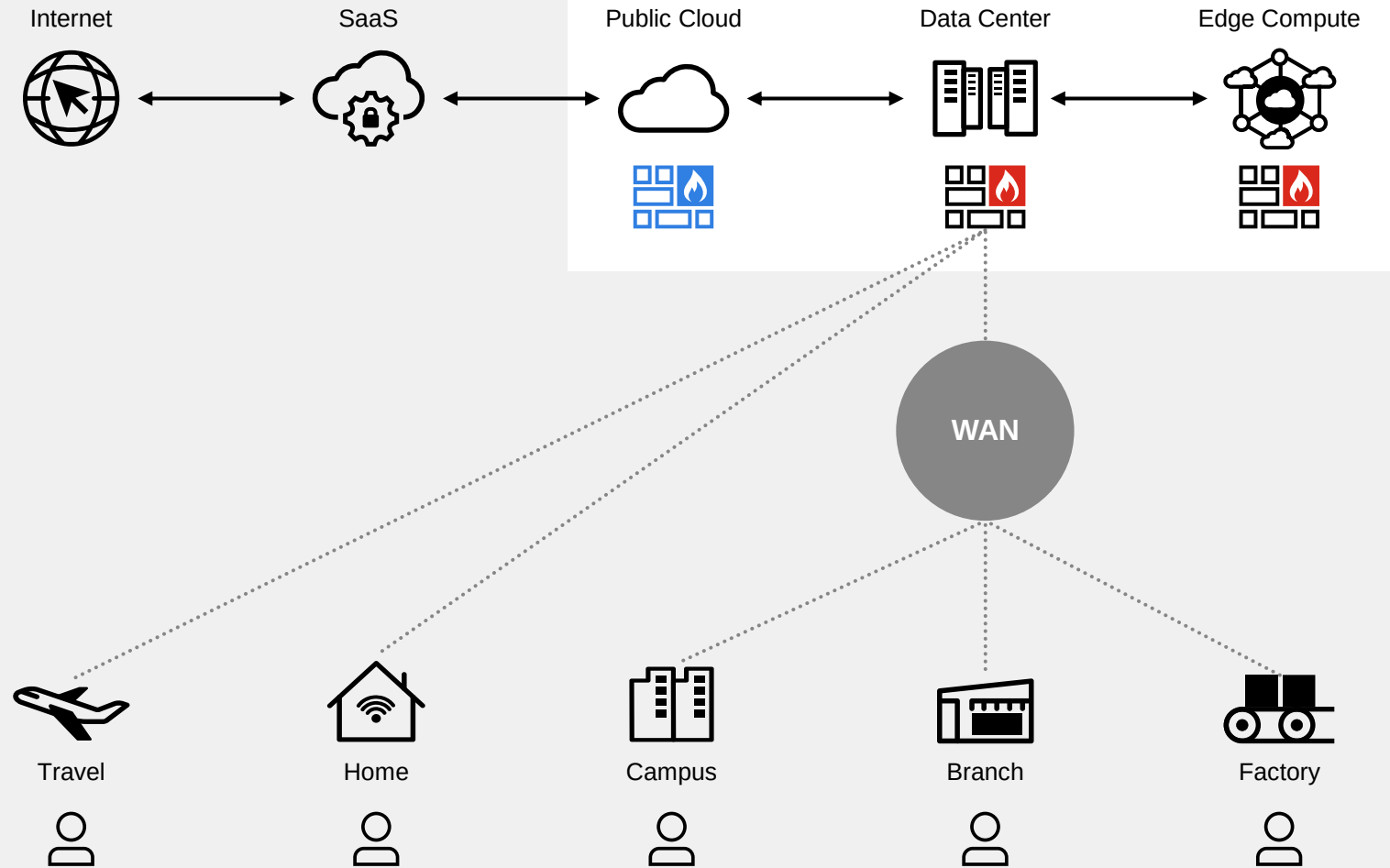
Сегментована

З захищеними сервісами

З захищеним інтернетом

Розшифровка трафіку

VPN



Етап 2: Додаємо можливості SD-WAN

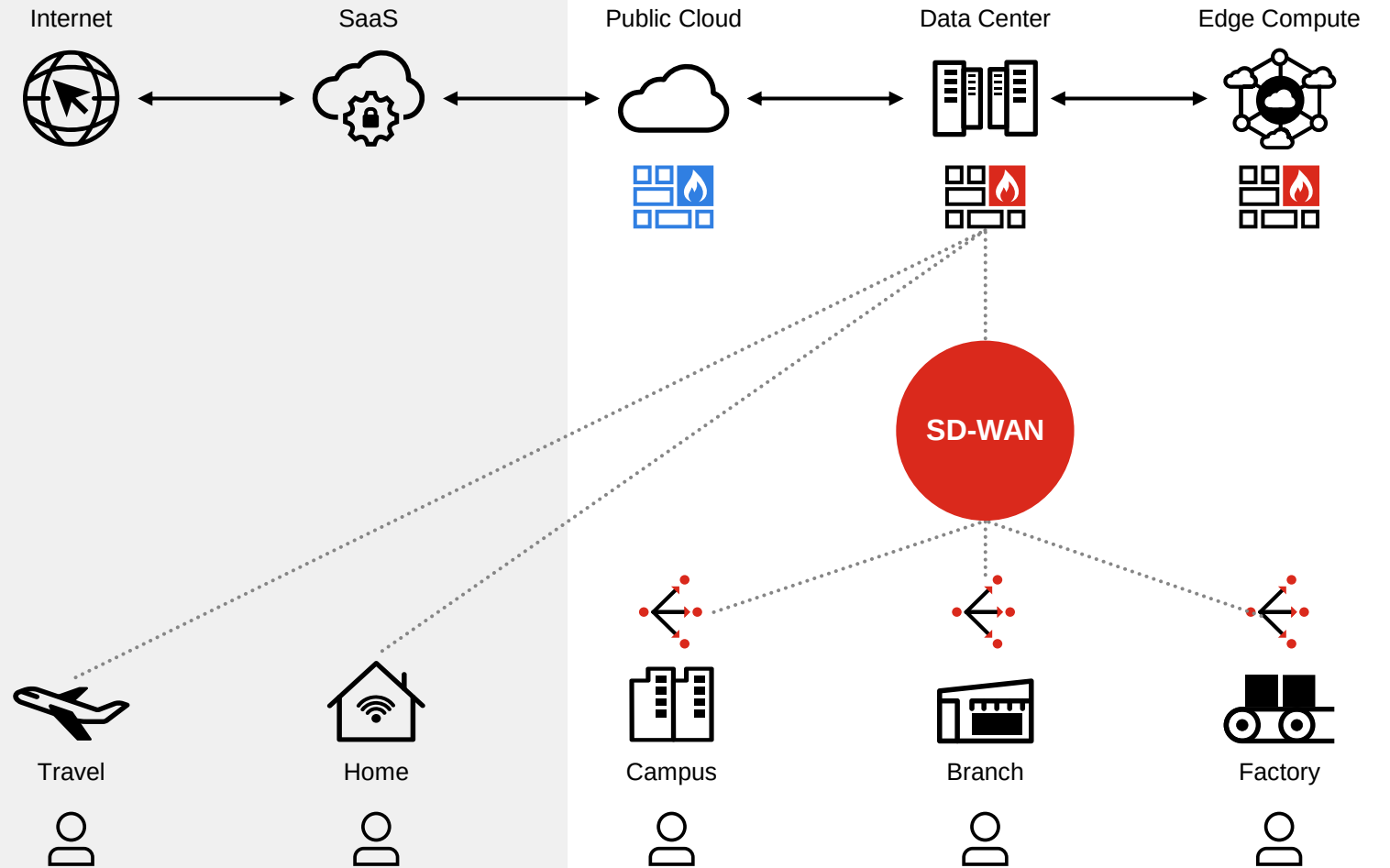
Динамічне керування трафіком

Пріорітезація на основі сервісу

Висока доступність

Підтримка бездротових каналів зв'язку в якості резерву

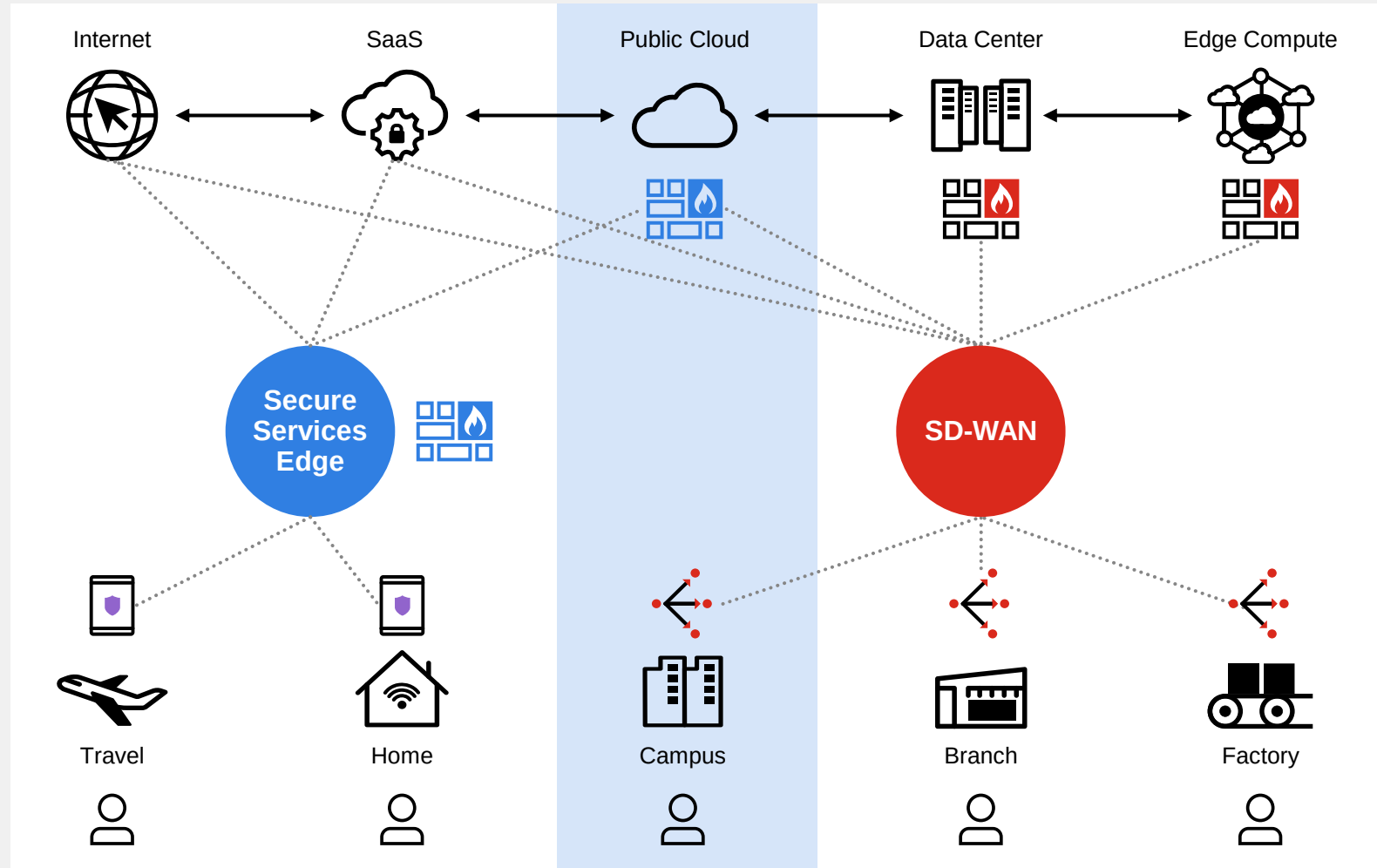
Контроль швидкості та якості



Етап 3: Користувачі що працюють віддалено

Віддалені користувачі переходять на SASE Cloud

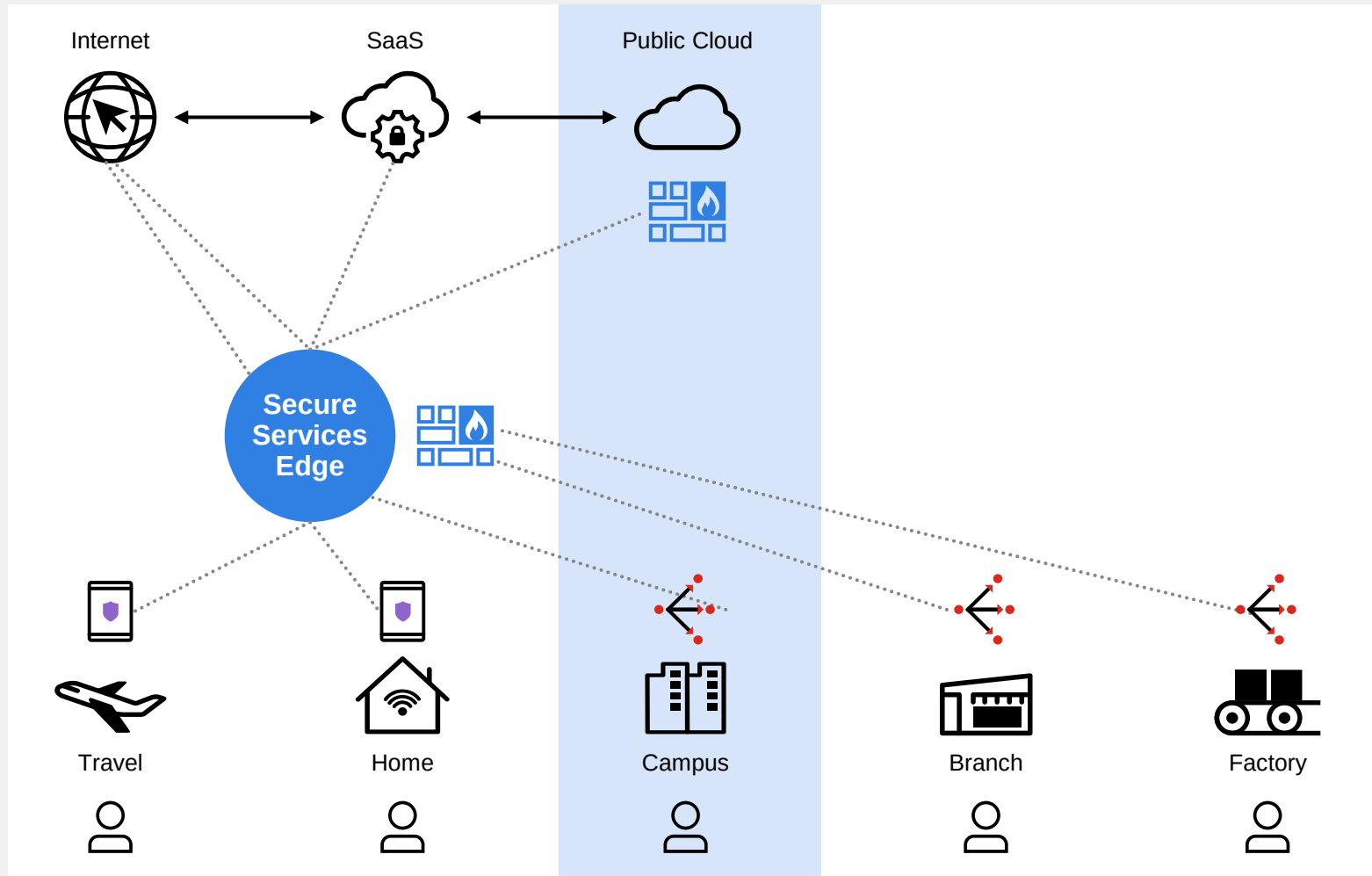
- FWaaS
- SWGaaS
- CASB



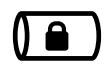
Етап 4: Відмова від локального ДЦ

Весь трафік обробляється та термінується в хмарі

Безпека забезпечується SASE хмарию у зв'язці з наземним обладнанням що лишилась



Основні задачі для SASE



Доступ до
сервісів



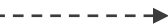
Традиційний VPN



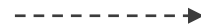
ZTNA



Internet захист
до сервісів в т.ч.
SaaS



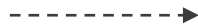
Традиційний Proxy



SWG, CASB



Модернізація
мережі



Маршрутизатор



Secure SD-WAN

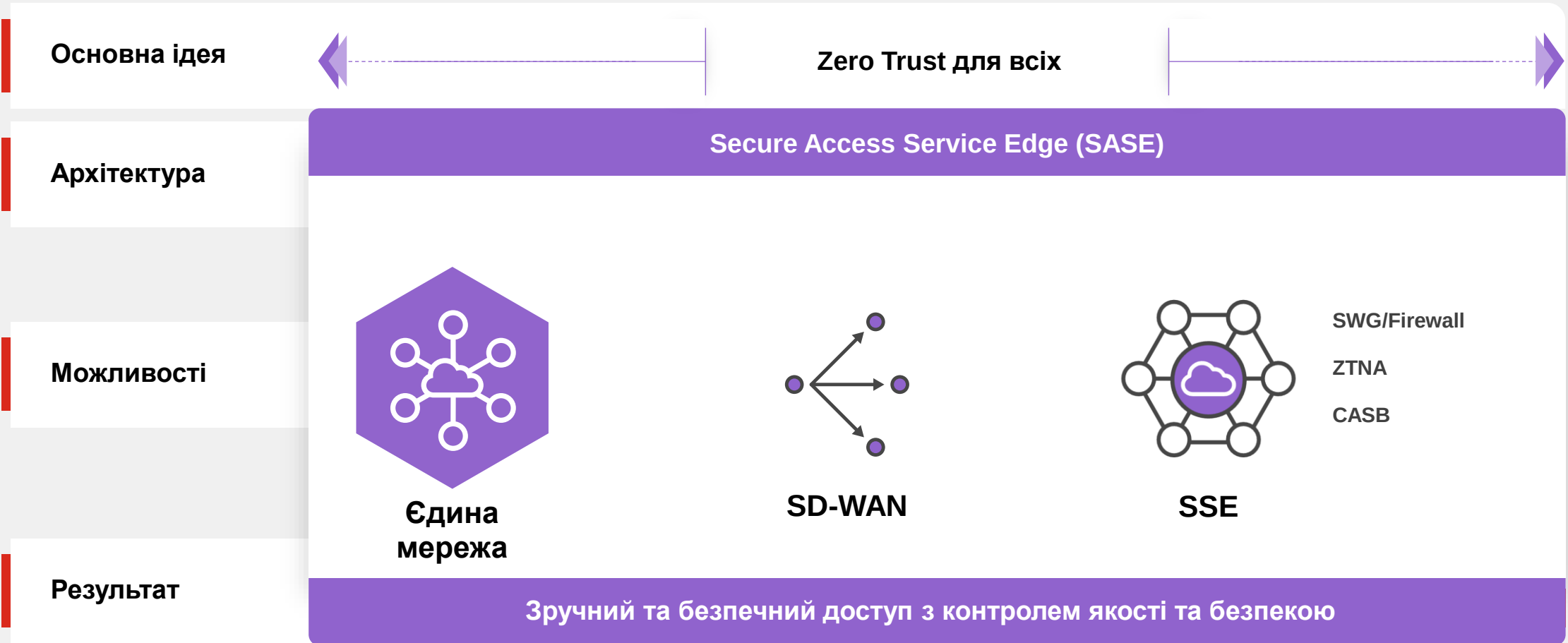


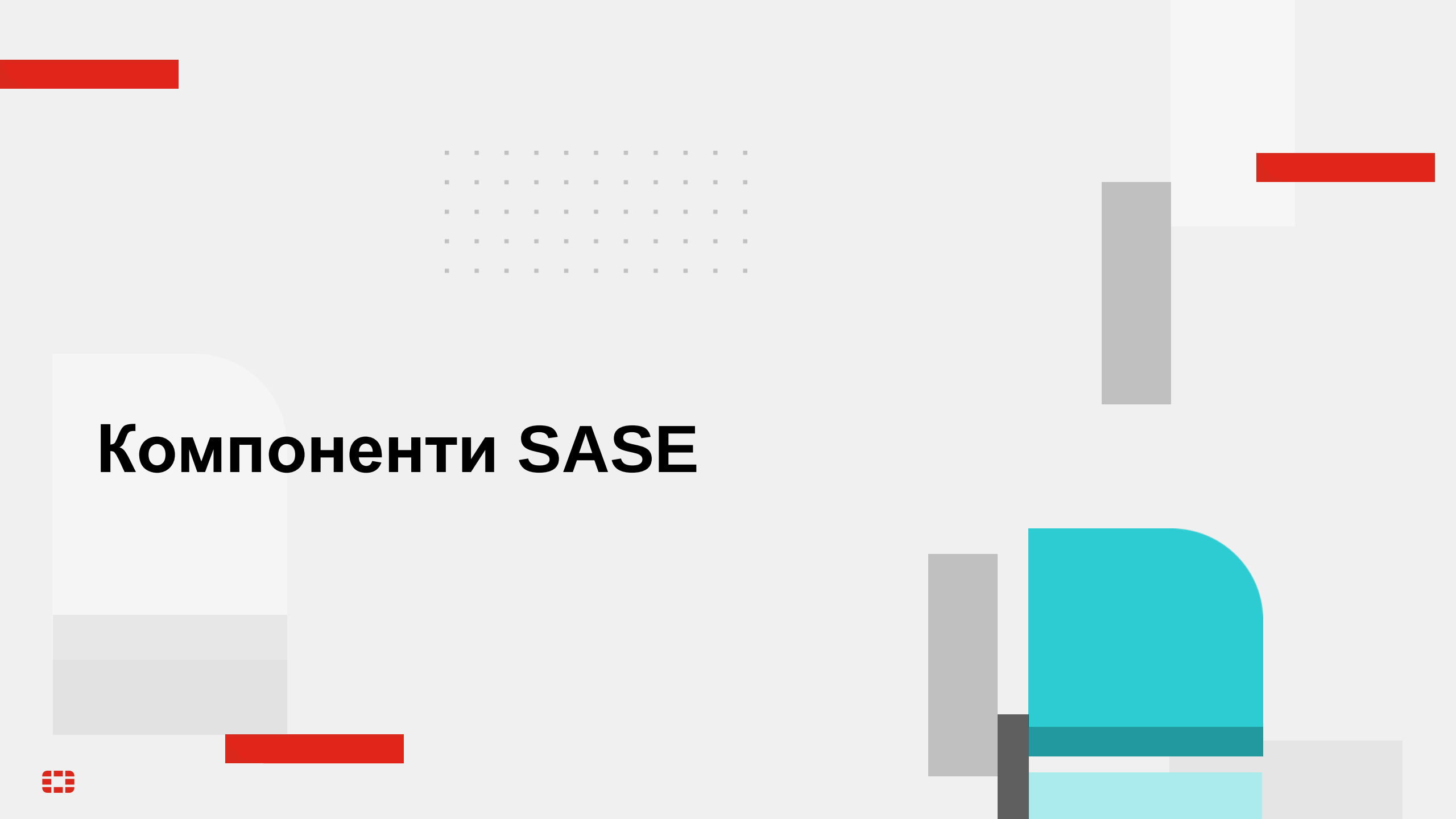
65%

Планують розглянути
SASE протягом року



SASE як основа для безпечного доступ



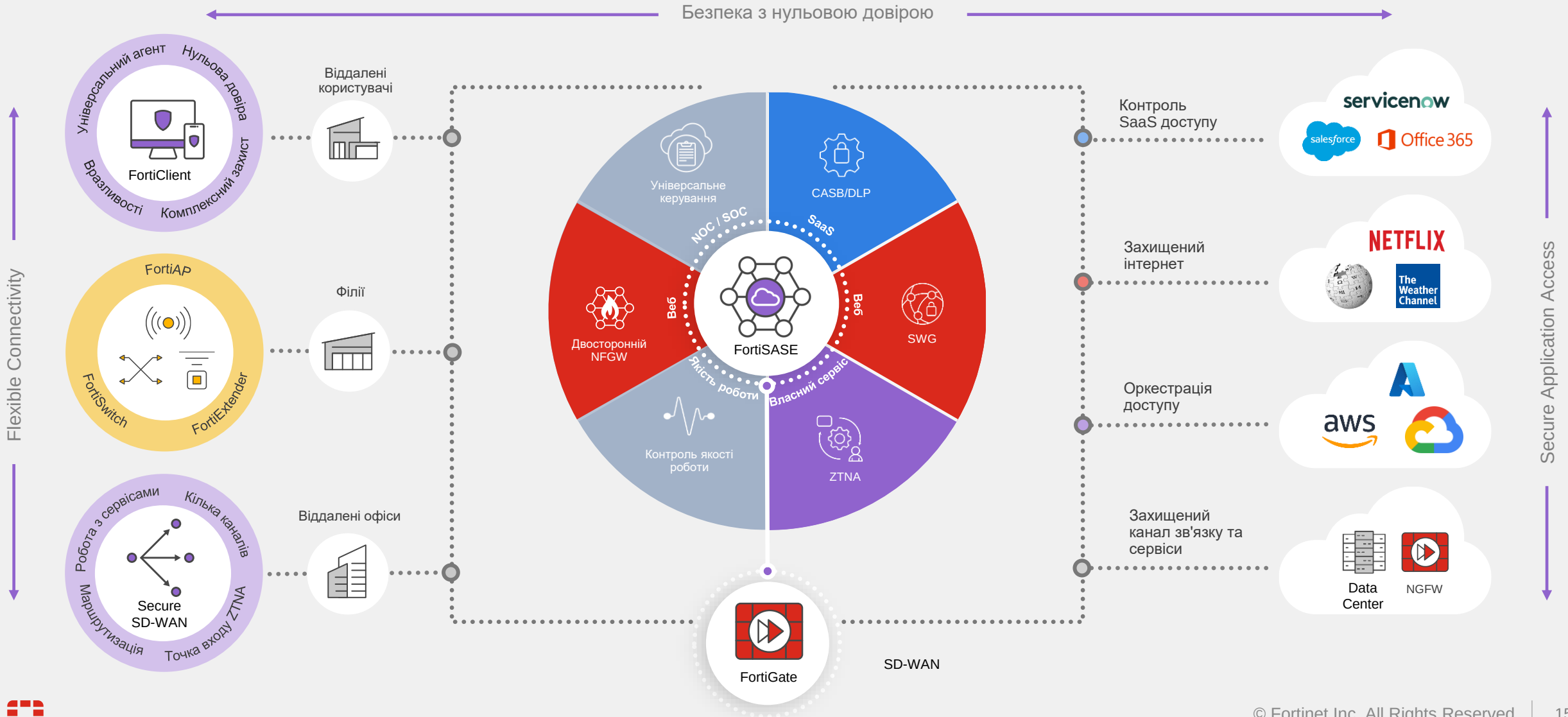


Компоненти SASE



Fortinet Universal SASE

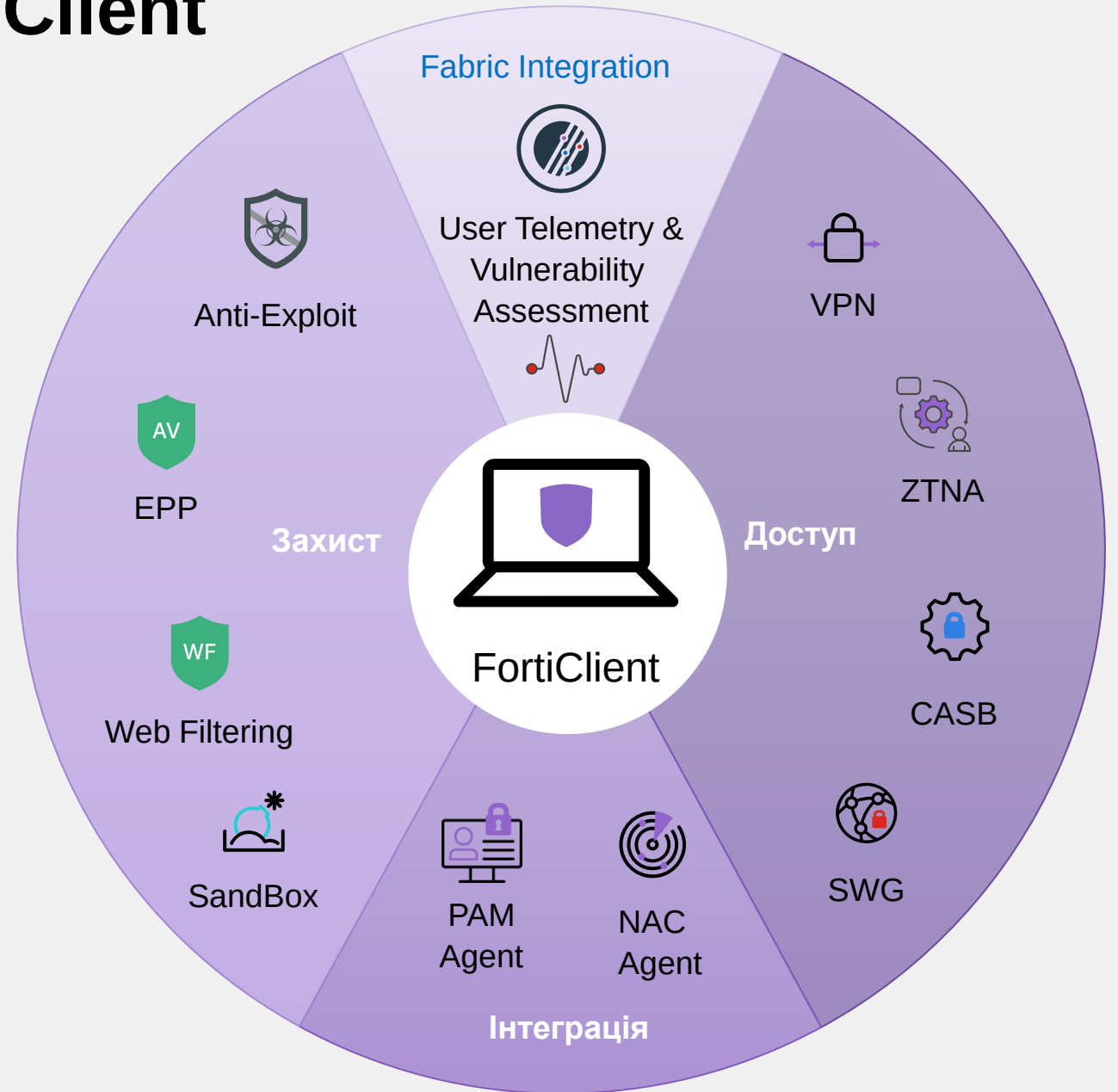
Перевірена безпека та зв'язок усюди



Уніфікований агент - FortiClient

Один агент для всего*

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



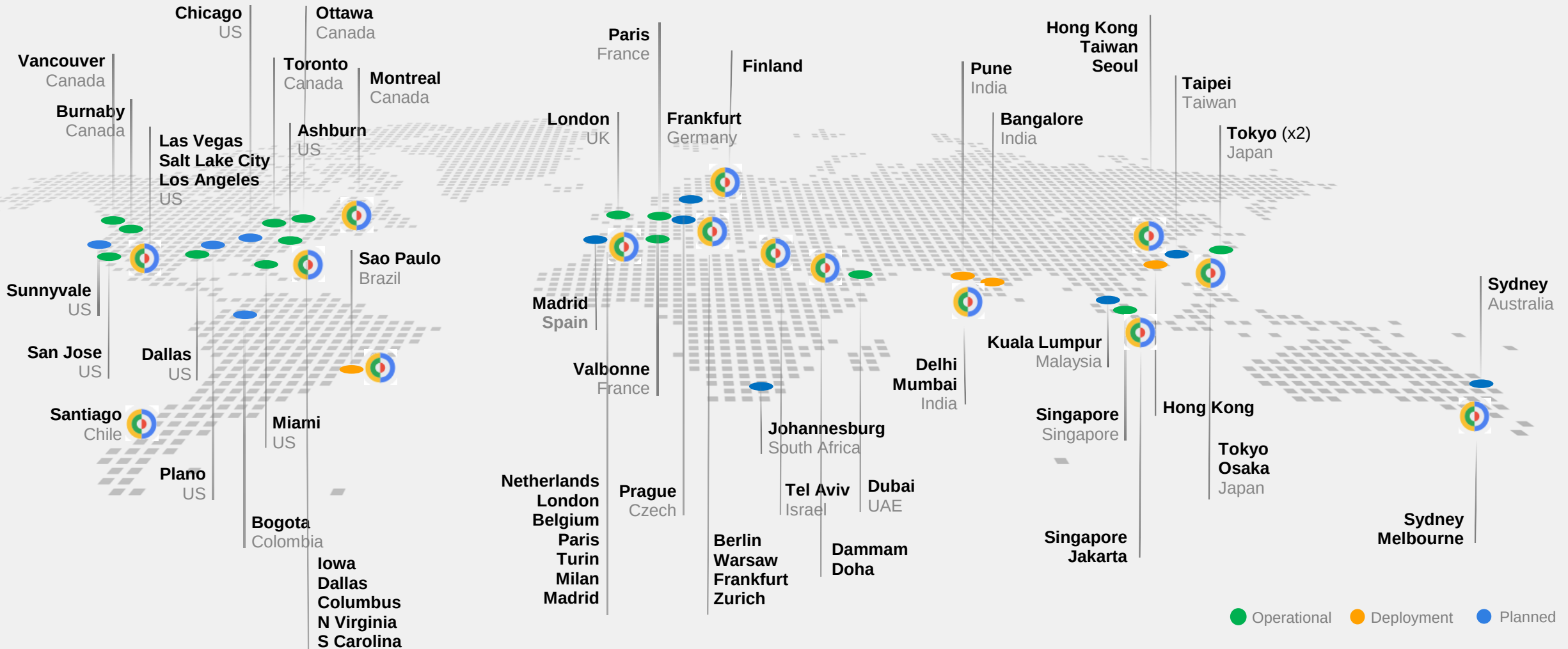
Точки присутності

Глобально

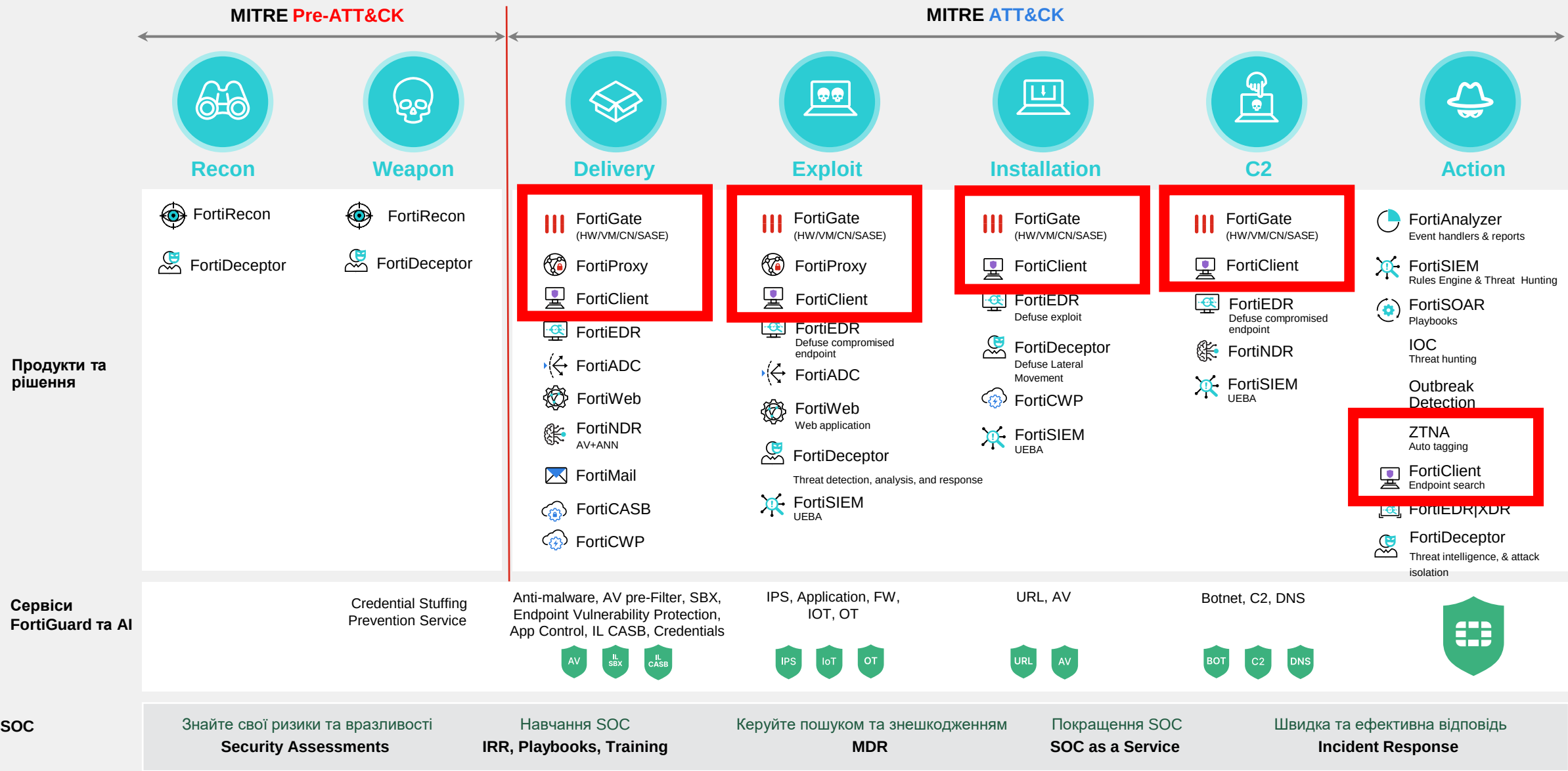
90+ локацій

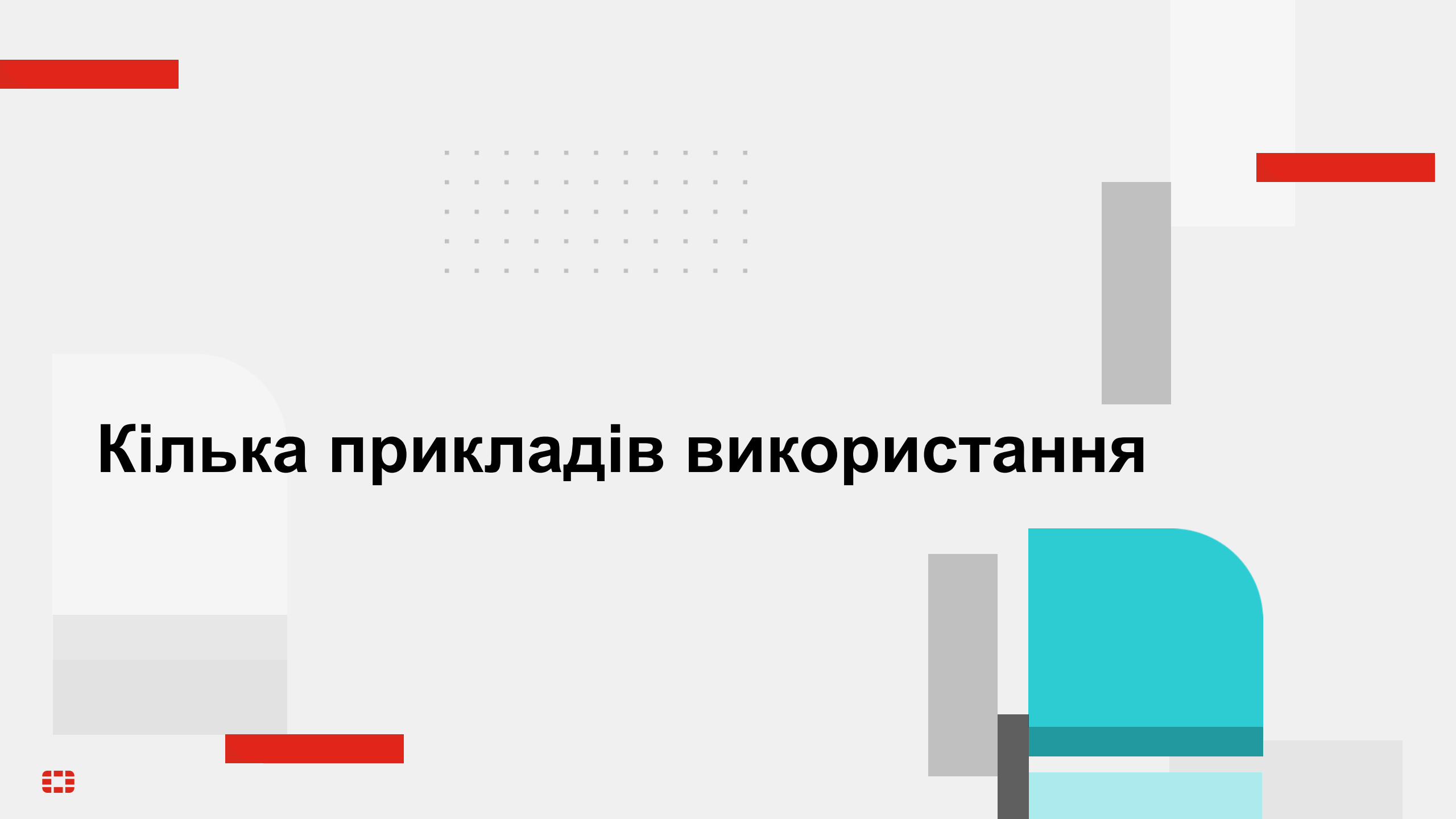
Безпека як сервіс

Низькі затримки з
високим SLA



Комплексний підхід до безпеки





Кілька прикладів використання

Безпечний Інтернет для співробітників

Для офісів та віддалених співробітників

Безпечний Інтернет



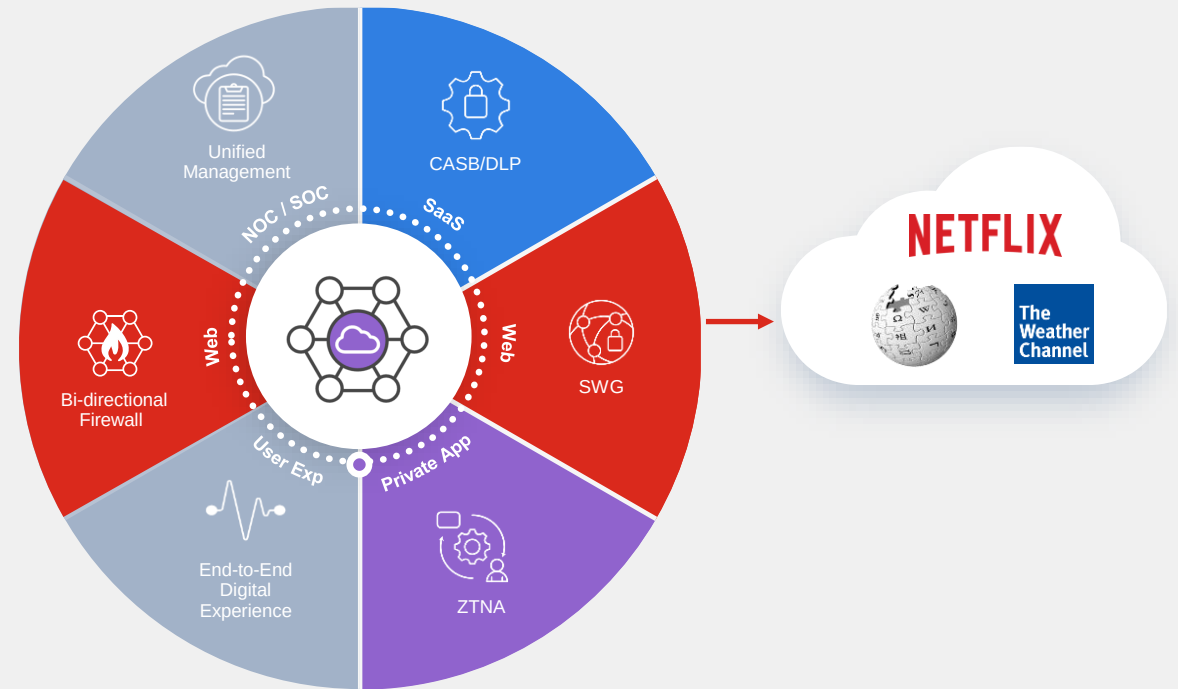
Захист від Malware & ransomware
Постійна оцінка вразливостей та протидія



Глибока перевірка трафіку
Постійна перевірка веб сайтів навіть коли використовується HTTPS



Перевірене рішення
FortiGuard Labs перевірений як тестами так і ринком



Безпечний Інтернет – Захист

The screenshot displays the FortiSASE Security configuration page. The left sidebar shows the 'Security' menu item highlighted with a red box and a red circle containing the number 1. The main content area is divided into several sections, each with a 'View All' and 'View Logs' button. The sections are: AntiVirus, Web Filter, Intrusion Prevention, File Filter, Data Leak Prevention, DNS Filter, Application Control With Inline-CASB, and SSL Inspection. The top right of the interface shows a 'Profile Group' dropdown menu with 'Default' selected, and two buttons: 'Internet Access' and 'Private Access', both highlighted with red boxes and red circles containing the number 2. The 'DNS Filter' section has a 'Customize' button highlighted with a red box and a red circle containing the number 4. The 'Intrusion Prevention' section has a 'Recommended' action button highlighted with a red box and a red circle containing the number 3.

Section	Threats	Count	Filters
AntiVirus	No Data		
Web Filter	dns.google	214	Allow 1
Web Filter	clientservices.googleapis.com	48	Block 23
Web Filter	spclient.wg.spotify.com	48	Exempt 0
Web Filter	safebrowsing.googleapis.com	48	Monitor 73
Web Filter	173.243.138.98	39	Warning 0
Web Filter			Disable 0
Intrusion Prevention	No Data		
File Filter	live-tile-xml	48	Block 2
File Filter	update2	10	Monitor 54
File Filter	hfnkpmihhgieaddgfemjhof...	1	
File Filter	hfnkpmihhgieaddgfemjhof...	1	
File Filter	e6c1c50b923d3da4ddb13...	1	
Data Leak Prevention	data leak by filter: SSN Info	2	
Data Leak Prevention			Allow 0
Data Leak Prevention			Block 0
Data Leak Prevention			Monitor 2
DNS Filter	No Data		
DNS Filter			Allow 65
DNS Filter			Block 9
DNS Filter			Monitor 17
Application Control With Inline-CASB	QUIC	24	
Application Control With Inline-CASB			Allow 0
Application Control With Inline-CASB			Block 1
Application Control With Inline-CASB			Monitor 19
SSL Inspection	ssl-anomaly	6	
SSL Inspection			Deep Inspection
SSL Inspection			SSL connections are decrypted to allow for inspection of the contents.
SSL Inspection			Exempt Hosts 1
SSL Inspection			Exempt URL Categories 2

- 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



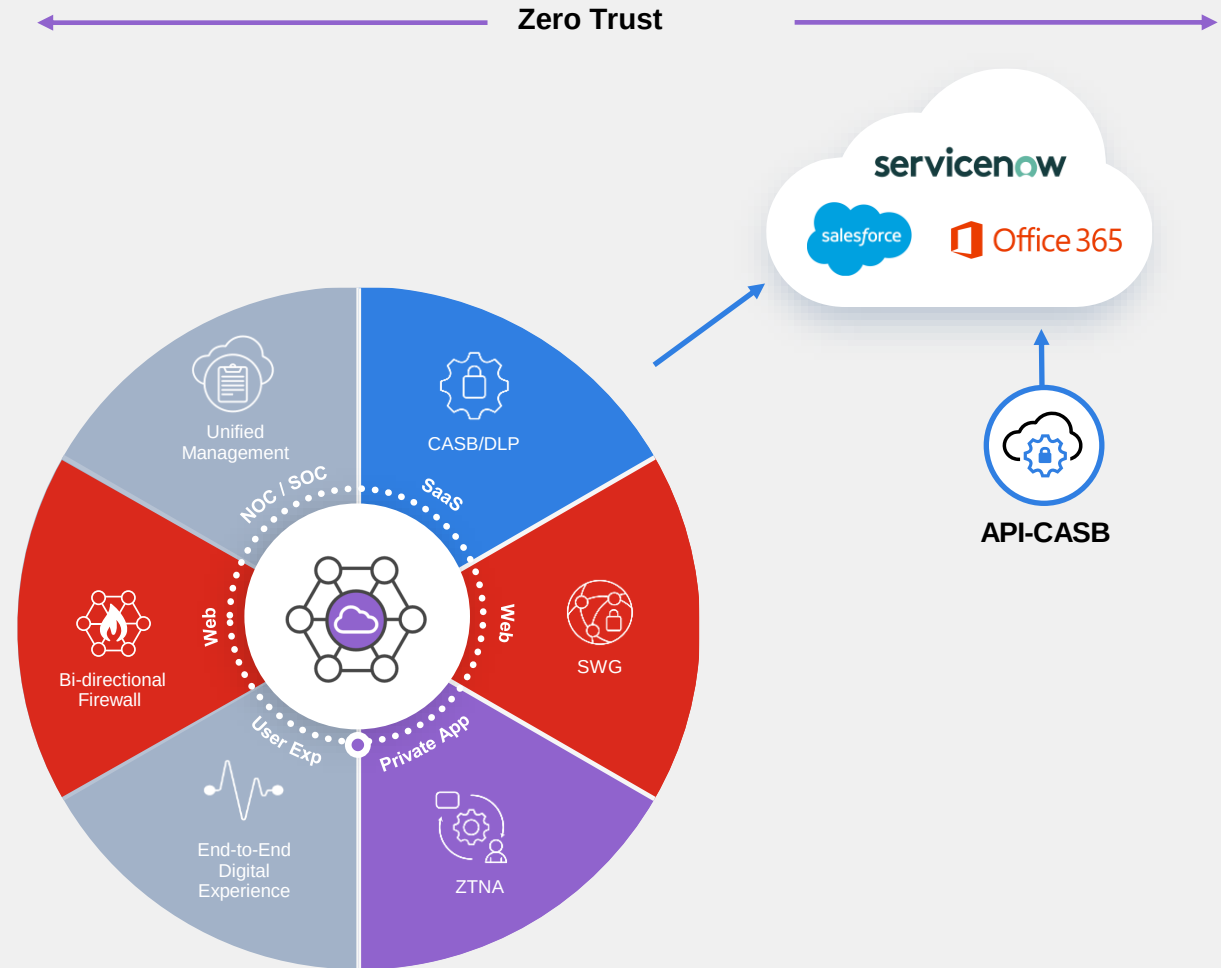
Контроль та перегляд вмісту

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

The screenshot displays the FortiSASE Security dashboard. The left sidebar contains navigation options: Dashboards, Network, Configuration, Security (highlighted with a red box), RESOURCES, Hosts, Services, ACCESS, Users, AUTHENTICATION SOURCES, LDAP, RADIUS, VPN User SSO, SWG User SSO, ENDPOINTS, Profile, ZTNA Tagging, ZTNA Access Proxies, System, and Analytics. The main content area shows several security modules:

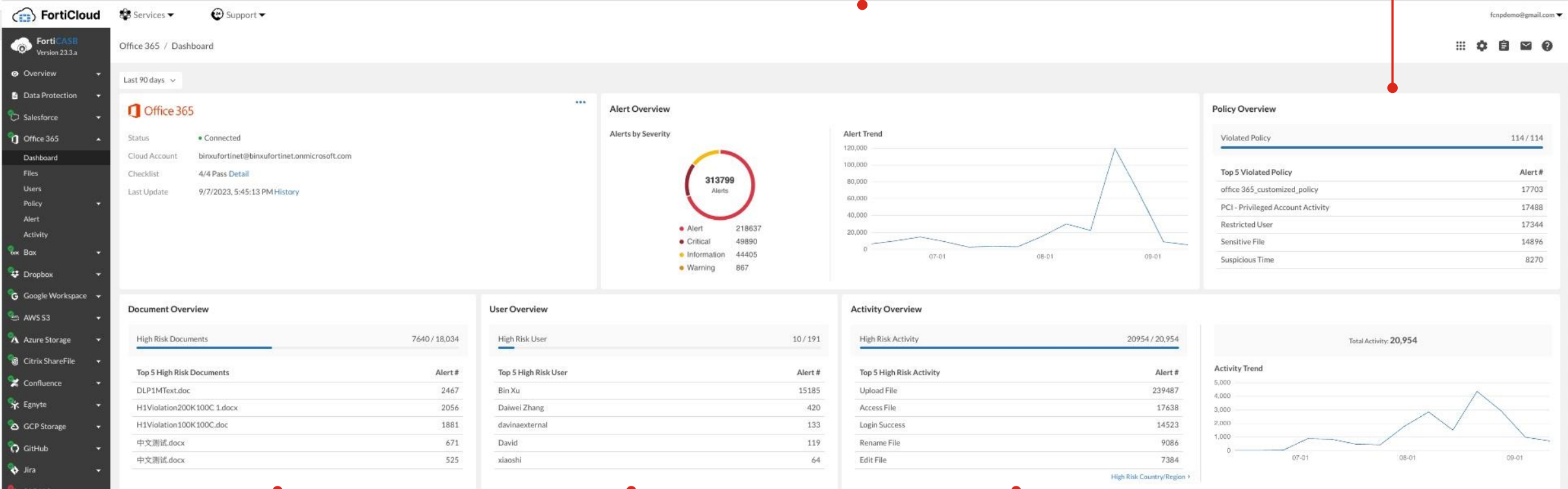
- Internet Access**: A table with columns 'Threats' and 'Count'. It lists several threats with counts of 1. A 'Monitor' button is visible.
- Data Leak Prevention**: A table with columns 'Threats' and 'Count'. It shows 'No Data'.
- DNS Filter**: A table with columns 'Threats' and 'Count'. It shows 'technitium.tmlab.network' with a count of 25. A 'Monitor' button is visible.
- Application Control With Inline-CASB** (highlighted with a red box): A table with columns 'Threats' and 'Count'. It shows 'No Data' and a warning message: '110 Cloud Applications can be monitored & controlled by Inline-CASB when SSL inspection is enabled.' A 'Monitor' button is visible.
- SSL Inspection**: A table with columns 'Threats' and 'Count'. It shows 'No Data' and a 'Certificate Inspection' section with a message: 'SSL certificates are inspected to categorize traffic. No decryption of traffic is performed.'

- 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

The screenshot displays the FortiCloud Shadow IT Application List interface. The sidebar on the left contains navigation options: Overview, Dashboard, Report, Audit Log, Shadow IT, and Dashboard. The main content area is titled 'Shadow IT Application List' and includes a 'Score' slider (0 to 100) and a 'Categories' list with checkboxes for various application types. The table on the right lists applications with columns for Application, Category, Risk Score, Number of Clients, and Sessions (Blocked/Allowed). The Risk Score column is highlighted with a red box, and the filter section is also highlighted with a red box.

Application	Category	Risk Score	Number of Clients	Sessions (Blocked/Allowed)
Harris Media	Web Hosting	98	1	140 (0 / 140)
Hosting.India.to	Web Hosting	88	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	66	1	2 (0 / 2)
GalaxyHostPlus	Web Hosting	64	1	2 (0 / 2)
FarmLogs	Inventory & SCM	63	1	3 (0 / 3)
Host.ag	Dedicated Hosting	61	1	5 (0 / 5)
Azendoo	Project Management Tools	57	1	5 (0 / 5)
http://host.co.in	Dedicated Hosting	54	1	3 (0 / 3)
DigitalOcean	Cloud Hosting	52	1	10 (0 / 10)
Baidu Cloud	Cloud Hosting	38	1	35 (0 / 35)
box	Online Backup	18	1	1 (0 / 1)
AWS	Cloud Hosting	10	2	269 (0 / 269)
Bizible	Marketing Software	8	1	1 (0 / 1)
CloudFlare	Cloud Hosting	6	1	1 (0 / 1)
Data.com	Operations Management	5	2	1722 (259 / 1463)
Digital Global Hosting	Web Hosting	0	1	6 (0 / 6)
Do	Project Management Tools	0	2	13 (0 / 13)



Гібридна інфраструктура. Наступний рівень.

Разом з ZTNA та SD-WAN

Доступ до внутрішніх сервісів



Безпечний доступ в хмару/ЦОД

Захищений доступ до сервісів



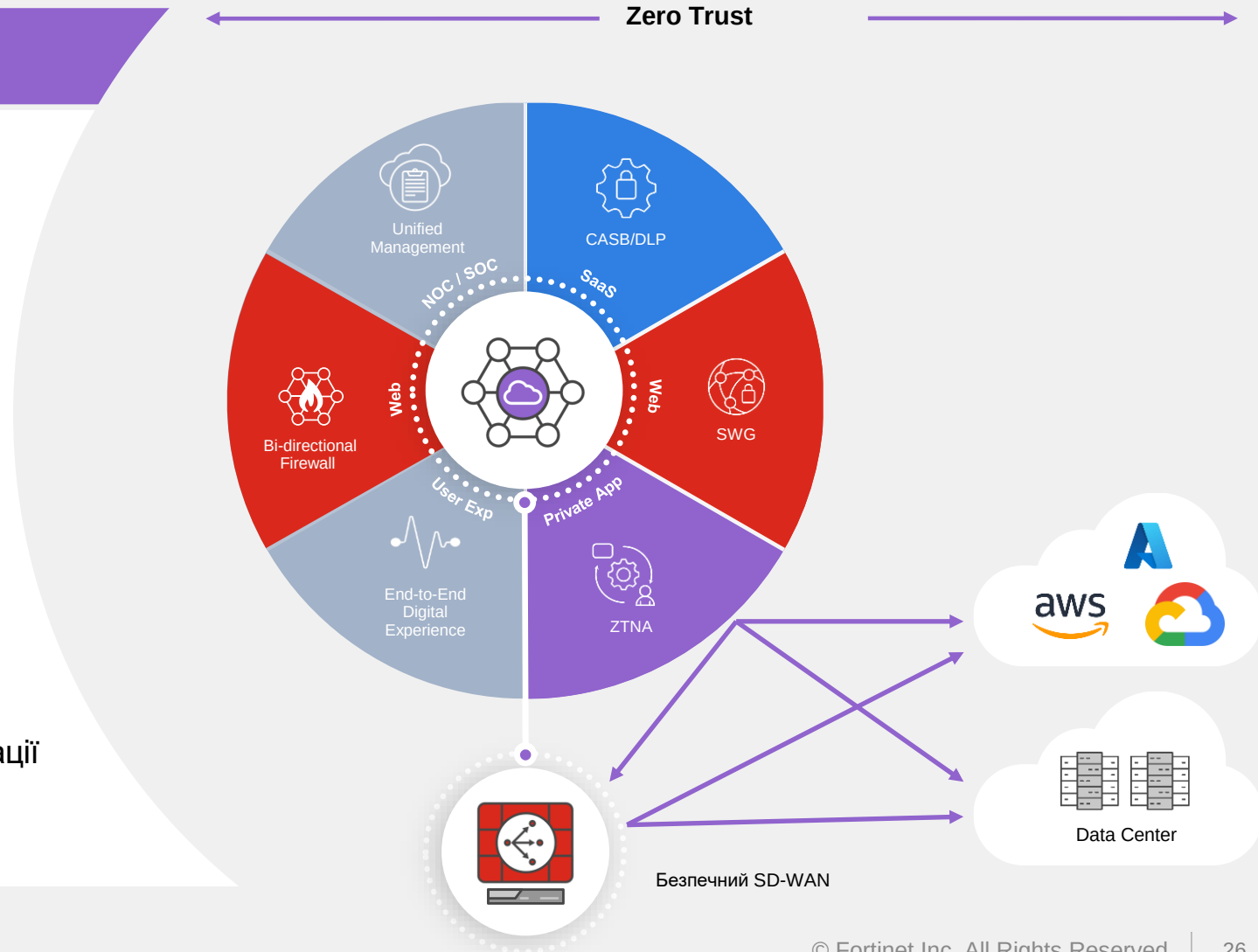
Детальний контроль доступу

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



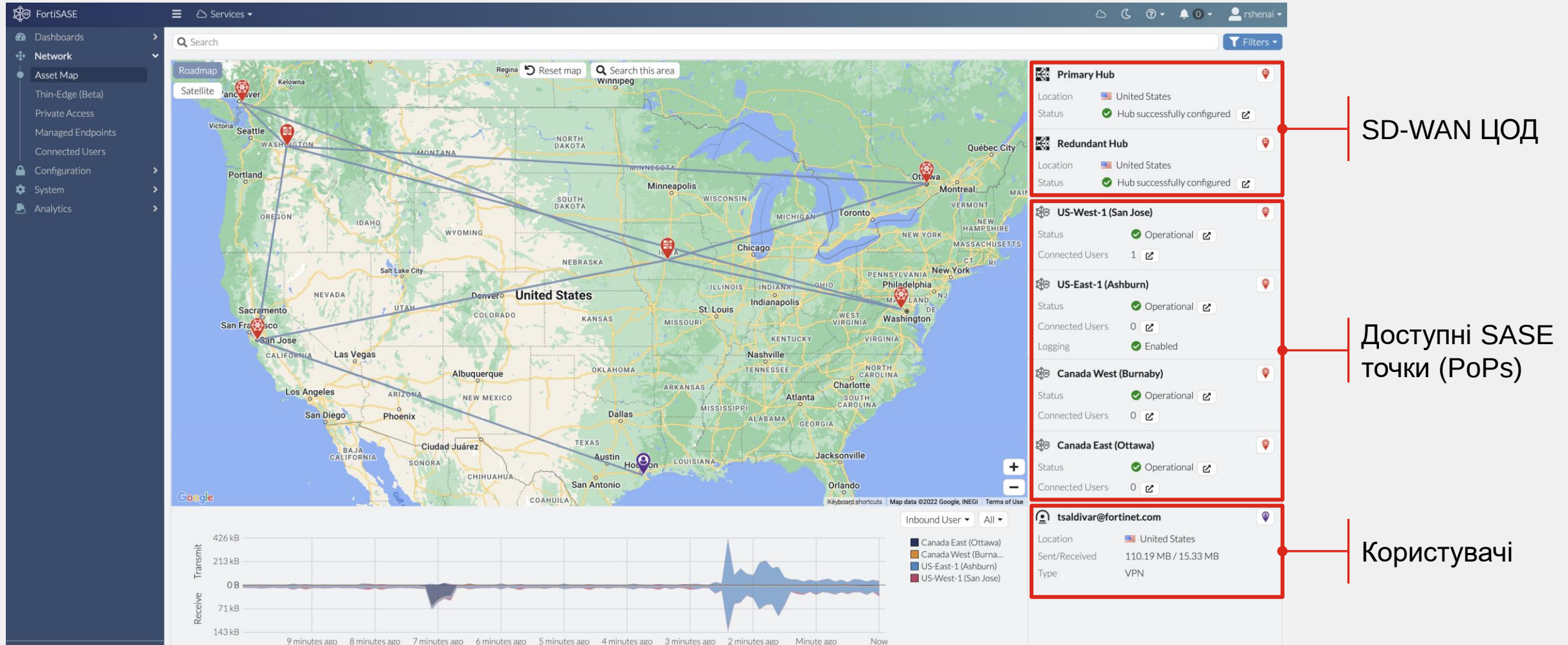
Інтеграція з існуючим SD-WAN

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



FortiSASE SPA

Прозоре та безпечне підключення користувачів до їх сервісів



Zero Trust безпека для сервісів

Аутентифікація | Централізоване керування | Постійні перевірки

The screenshot displays the FortiSASE console interface for configuring Zero Trust Network Access (ZTNA) rules. The interface is divided into several sections:

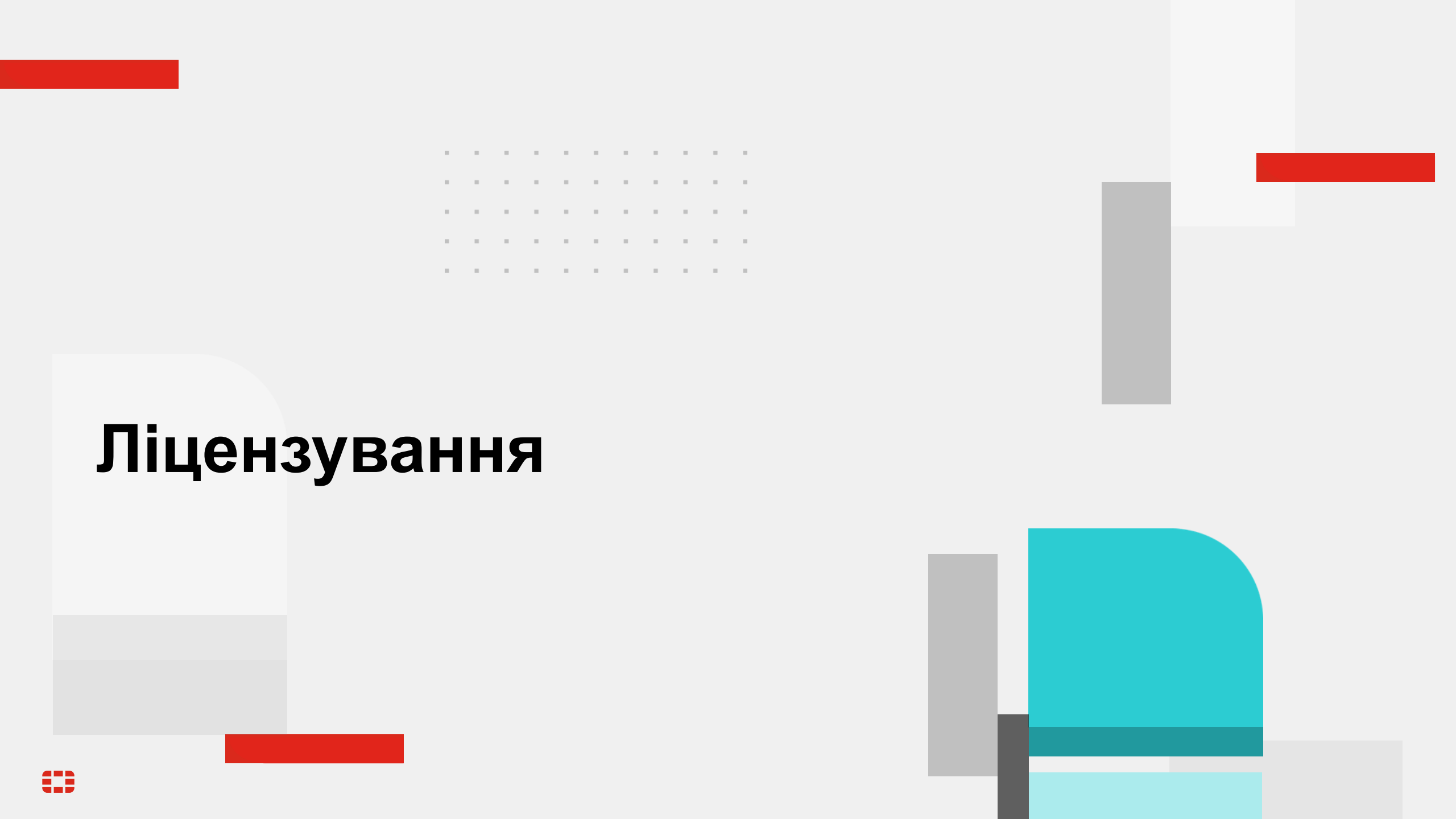
- Left Sidebar:** Contains navigation menus for Dashboards, Network, Configuration, TRAFFIC, Policies, SWG Policies, Security, NETWORK, DNS, RESOURCES, Hosts, Services, ACCESS, Users & Groups, PKI, AUTHENTICATION SOURCES, LDAP, RADIUS, VPN User SSO, SWG User SSO, ENDPOINTS, Profiles, ZTNA Tagging, ZTNA Access Proxies, and Analytics. Red boxes and numbers highlight specific areas: (1) Profiles, (2) ZTNA Tagging, and (3) Policies.
- Main Configuration Area:** Titled "CREATE RULE SET", it includes fields for Name, Enabled (toggle), and Comments. Below this, there are sections for "When the following rules match" and "Apply the following tag". A red box and number (1) highlight the "Create ZTNA Connection Rule" section, which includes fields for Rule Name, Destination Host, ZTNA Access Proxy, Encryption (toggle), and Use External Browser for SAML Authentication (toggle).
- Operating System Selection:** A dropdown menu for "Operating System" is shown, with tabs for Windows, macOS, Linux, iOS, and Android. A red box and number (2) highlight the "Rule Type" dropdown, which lists various security rules including AntiVirus, User in AD Group, Certificate, Domain, EMS Management, File, IP Range, OS Version, Registry Key, Running Process, Sandbox, Severity Level, User Identity, Windows Security, and On-Fabric Status.
- Bottom Table:** A table listing existing rules with columns for Name, Profile Group, Source, User, Destination, Action, Hit Count, and Status. Red box and number (3) highlight the table header.

Name	Profile Group	Source	User	Destination	Action	Hit Count	Status
Block_Access		Vulnerable	All VPN Users	All Private Access Traffic	Deny	43,279	Enabled
Mobile_Private-Access	Mobile-SPA	Managed_iOS Managed_Android	All VPN Users	All Private Access Traffic	Accept	66,934	Enabled
SPA-Traffic	Default	Endpoint_Compliance Windows-Firewall_On Disk-Encryption-On	All VPN Users	All Private Access Traffic	Accept	72,367	Enabled
Allow-All Private Traffic Thin edge	Default	All Thin-Edge Devices		All Private Access Traffic	Accept	261	Enabled
Implicit Deny		all	All VPN Users	All Private Access Traffic	Deny	540,269	Enabled

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 Premium 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	✓	✓	✓
SASE Cloud Logging, Reporting & Alerting	✓	✓	✓
Digital Experience Monitoring		✓ ^③	✓ ^③
SOC-as-a-Service Integration		✓	✓
FortiGuard Forensics (Response) Service		✓ ^③	✓ ^③
Data Center			
Locations	Fortinet Cloud Locations	Fortinet Cloud Locations	Public Cloud Locations
Customer Support Services			
24x7 Premium Support	✓	✓	✓
Assisted On-boarding		✓	✓



Доп. опції

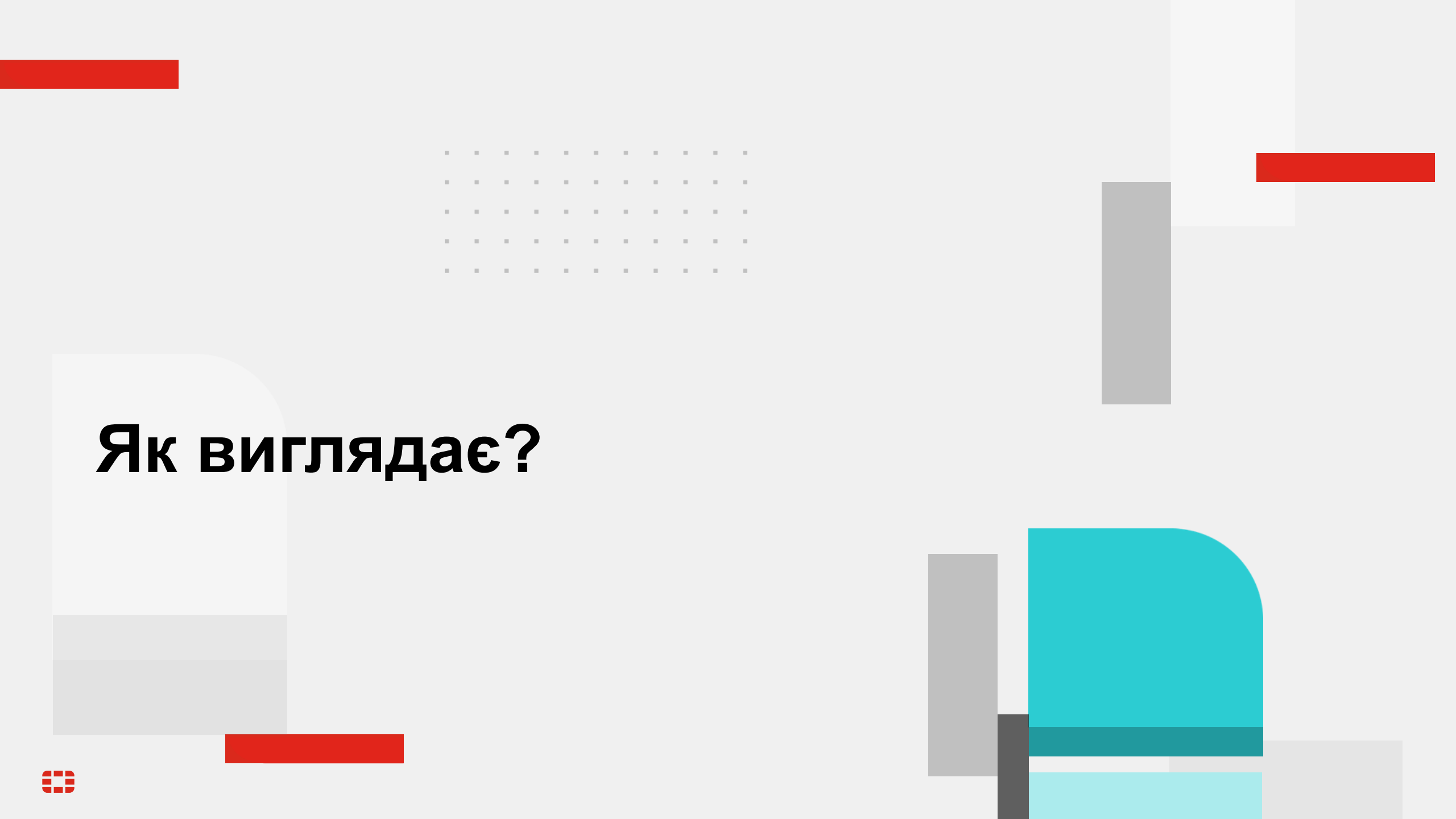
OPTION	QUANTITY
Bandwidth Add-on	25 Mbps
Dedicated Public IP Address	4 x Public IP Addresses
FortiGate SPA	License required per FortiGate
Fortinet Location Add-on	1 Location
Public Cloud Location Add-on	1 Location



Наявні FortiGate



			Bundles					
Service Category	Service Offering	A-la-carte	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							
	GeoIP DB Updates				included with FortiCare Subscription			
	Device/OS Detection Signatures							
	Trusted Certificate DB Updates							
	DDNS (v4/v6) Service							



Як виглядає?



ASSET MANAGEMENT

-  Dashboard
-  Products >
-  Marketplace >
-  Account Services

ASSETS & ACCOUNTS

-  Asset Management
-  FortiFlex
-  IAM

CLOUD MANAGEMENT

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



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

FortiSASE offers a global network of Tier 3+ data centers to secure remote user traffic and retain associated security logs.

Points of Presence (0/4)

Please select 4 data centers to host PoPs. Remote users are routed to available PoPs that are geographically closest to them.

Recommended Data Centers

- | | | | |
|---|--|---|--|
| ☐ Ashburn - Virginia - USA | ☐ Dallas - Texas - USA | ☐ Dubai - United Arab Emirates | ☐ Frankfurt - Germany |
| ☐ London - United Kingdom | ☐ Miami - Florida - USA | ☐ Paris - France | ☐ San Jose - California - USA |
| ☐ Singapore - Singapore | ☐ Sydney - Australia | ☐ Tokyo - Japan | ☐ Toronto - Canada |
| ☐ Vancouver - Canada | | | |

► Alternative Data Centers

Logging

Please select one data center to host the logging service. Once provisioned, the data center cannot be changed.

- | | | | |
|--|---|--|---|
| ☐ Ashburn - Virginia - USA | ☐ Dallas - Texas - USA | ☐ Dubai - United Arab Emirates | ☐ Frankfurt - Germany |
| ☐ London - United Kingdom | ☐ Miami - Florida - USA | ☐ Paris - France | ☐ San Jose - California - USA |
| ☐ Singapore - Singapore | ☐ Sydney - Australia | ☐ Tokyo - Japan | ☐ Toronto - Canada |
| ☐ Vancouver - Canada | | | |

FortiClient Endpoint Management

Endpoints will connect to this location through FortiClient to retrieve endpoint configuration and to validate licenses. Once provisioned, the location cannot be changed.

- | | | | |
|---|---|------------------------------------|--|
| ☐ Frankfurt - Germany | ☐ London - United Kingdom | ☐ Oregon - USA | ☐ Sydney - Australia |
| ☐ Tokyo - Japan | | | |

Continue

Стартове навчання

The screenshot displays the FortiSASE Onboarding interface. On the left, a sidebar lists various dashboards and monitors. The main content area is titled "FortiSASE Onboarding (1)" and features a list of onboarding steps. The first step, "VPN user single sign on (SSO) configuration", is currently selected and shows a video player. The video player displays the FortiSASE logo and the title "OnBoarding - Secure Internet Access part 1 of 3 - Authentication". Below the video player, there are buttons for "Back", "Next", and "Later".

FortiSASE Onboarding (1)

- 1** VPN user single sign on (SSO) configuration
 - Preparation
 - Video 02:41
 - Verify
- 2** User group, security profile group, and VPN policy configuration
 - Preparation
 - Video 03:14
 - Verify
- 3** Onboarding and connecting new users
 - Preparation
 - Video 02:24
 - Verify

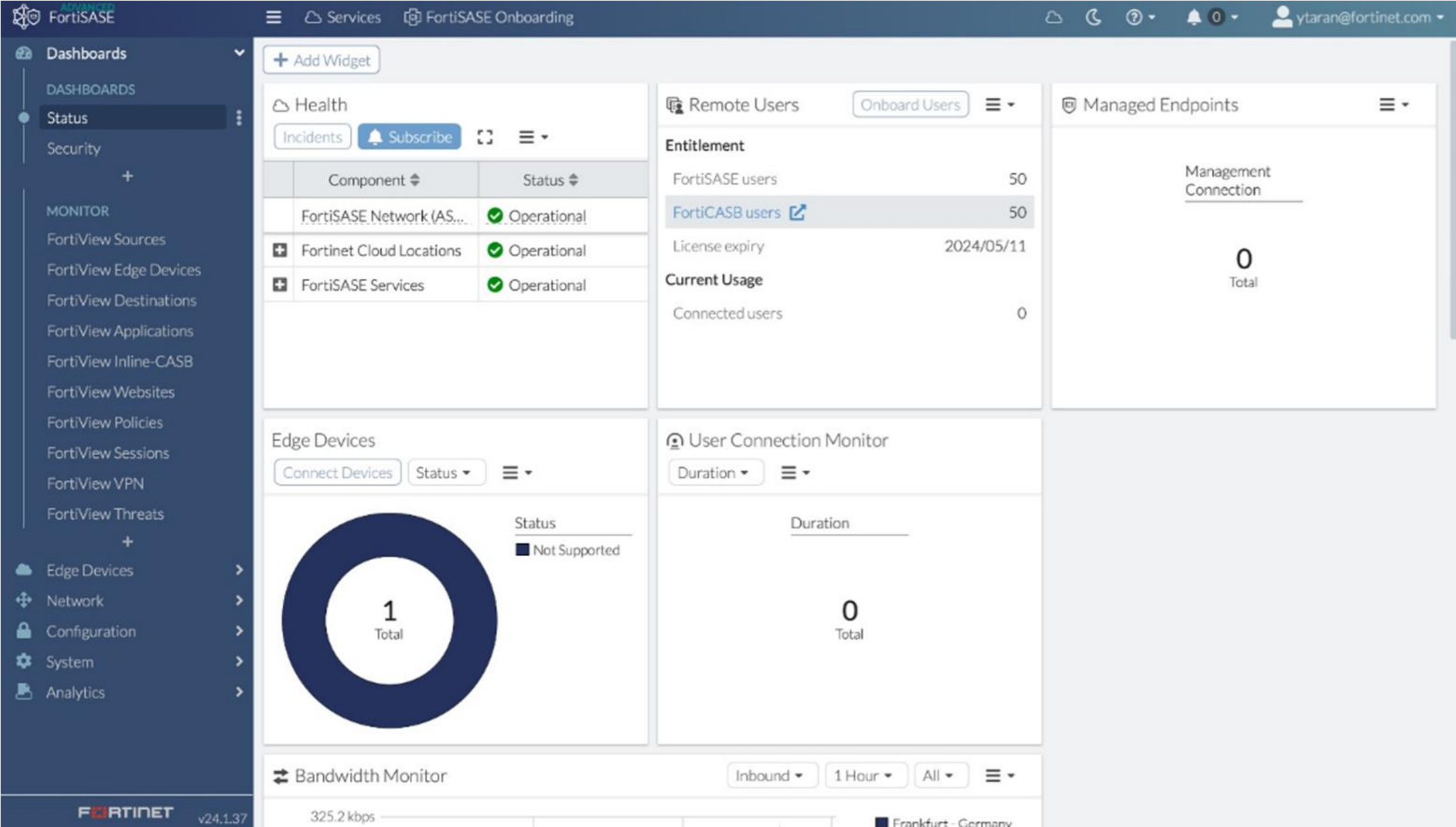
FortiSASE
Step-by-Step
OnBoarding - Secure Internet Access
part 1 of 3 - Authentication

02:41

Back Next Later



Перші кроки



Перші кроки

The screenshot displays the FortiSASE Onboarding interface. On the left is a dark sidebar with navigation options: Dashboards, MONITOR, and a bottom section with Edge Devices, Network, Configuration, System, and Analytics. The main area shows a 'Health' widget with a table of components (FortiSASE Network, Fortinet Cloud Locations, FortiSASE Services) all in 'Open' status. Below this is an 'Edge Devices' widget showing a donut chart with '1 Total' device. A 'Bandwidth Monitor' widget at the bottom shows '462.1 kbps'. A modal window titled 'Onboard Users' is open on the right. It contains instructions about endpoint management, a table for 'Managed Endpoint Users' (showing FortiClient Version 7.0.11), and options for downloading the FortiClient installer for Windows (x64), Linux, IOS, and Android. An invitation code is also displayed.

Onboard Users

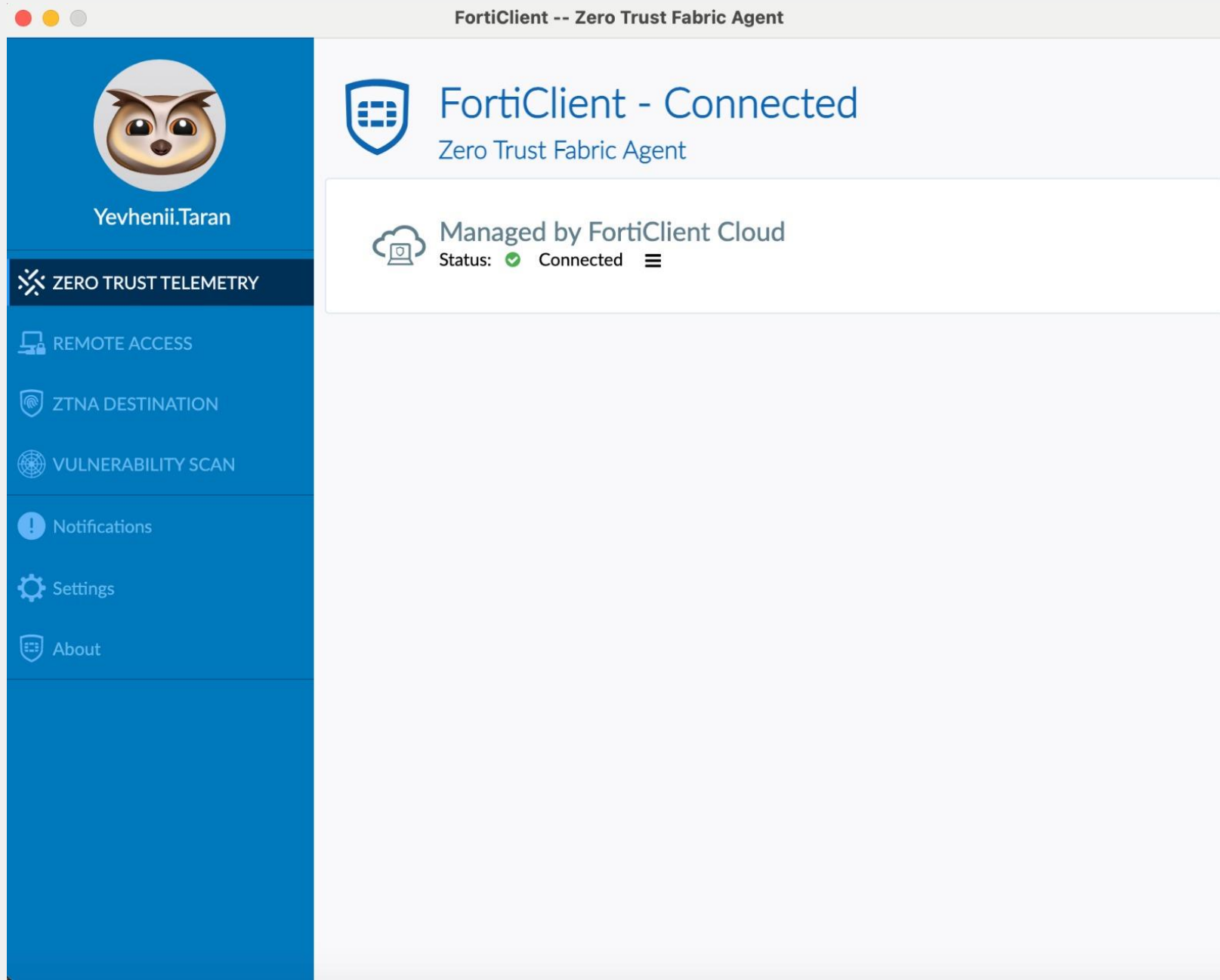
Endpoints managed by FortiClient connect to FortiSASE using VPN. Endpoints not managed by FortiClient connect using Secure Web Gateway.

Managed Endpoint Users	
FortiClient Version	7.0.11
FortiClient Installer	Download Send link to users
Preconfigured Installer	
OS	Windows (x64)
	Download Installer
Manual Installer <i>i</i>	
Invitation Code	IGKC84RQ4G3AHVTM7IINOC109PA2v <i>i</i>
Generic FortiClient Installers <i>i</i>	Linux IOS Android

[Close](#)



Перші кроки



Перші кроки

The screenshot displays the FortiSASE web interface. The left sidebar contains navigation menus for Dashboards, Monitor, and various system components. The main content area is divided into two sections: Internet Access Security Status and Vulnerability Summary.

Internet Access Security Status

Profile Group: Default | Internet Access

Security Feature	Status
AntiVirus	On (Red icon)
Web Filter With Inline-CASB	On (Blue icon)
Intrusion Prevention	On (Yellow icon)
DNS Filter	On (Green icon)
Application Control With Inline-CASB	On (Green 'A' icon)
SSL Inspection	On (Yellow padlock icon)

Vulnerability Summary

Vulnerability Level	Count	Category
Low	0	Third Party App
Medium	0	Service
High	1	Operating System
Critical	0	Web Client
	0	Microsoft Office
	0	User Config
	0	Other
Total	1	

Fortinet v24.1.37

Перші кроки

ADVANCED FortiSASE

ServicesFortiSASE 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

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

0

Low

1

Total

0

Third Party App

Internet Access Security

AntiVirus

Intrusion Prevention

Application Control

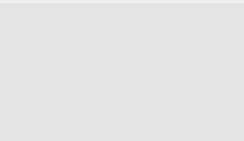
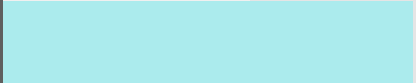
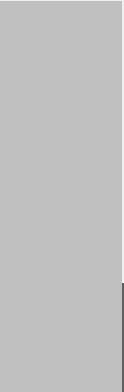
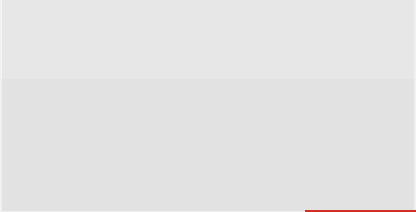
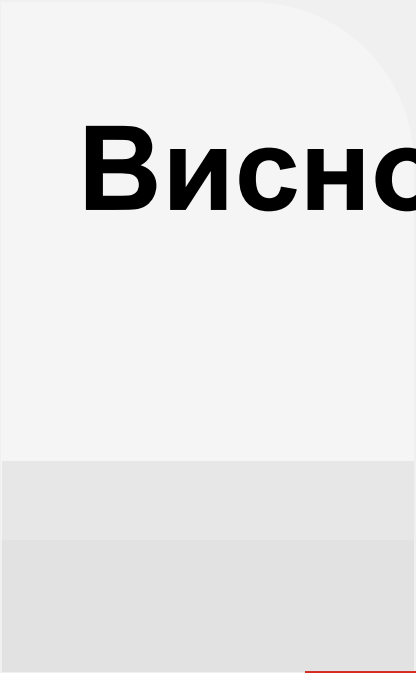
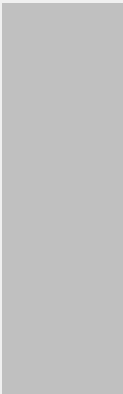
Vulnerability Summary

Fortinet

v24.1.1.37

1

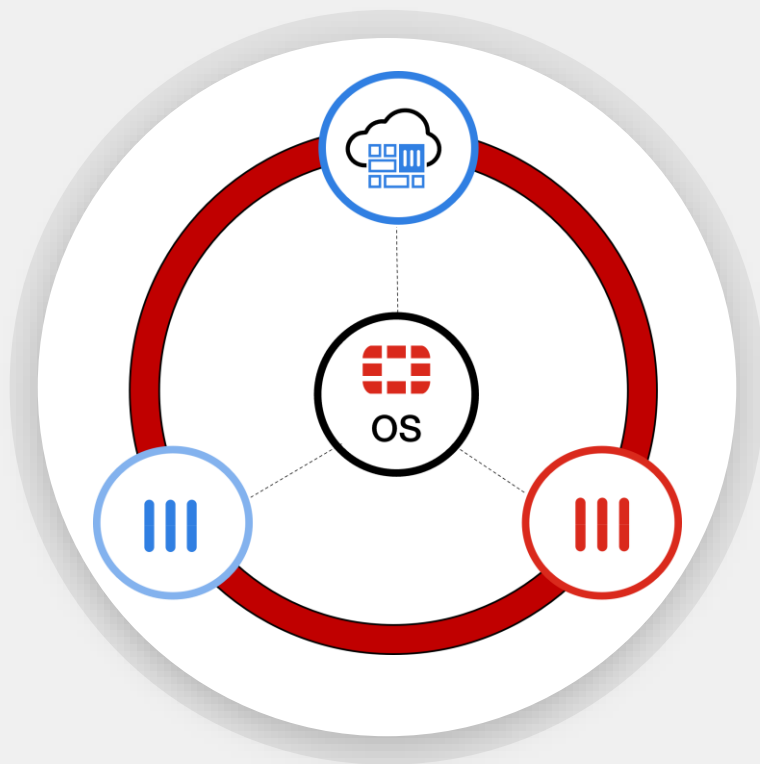
44



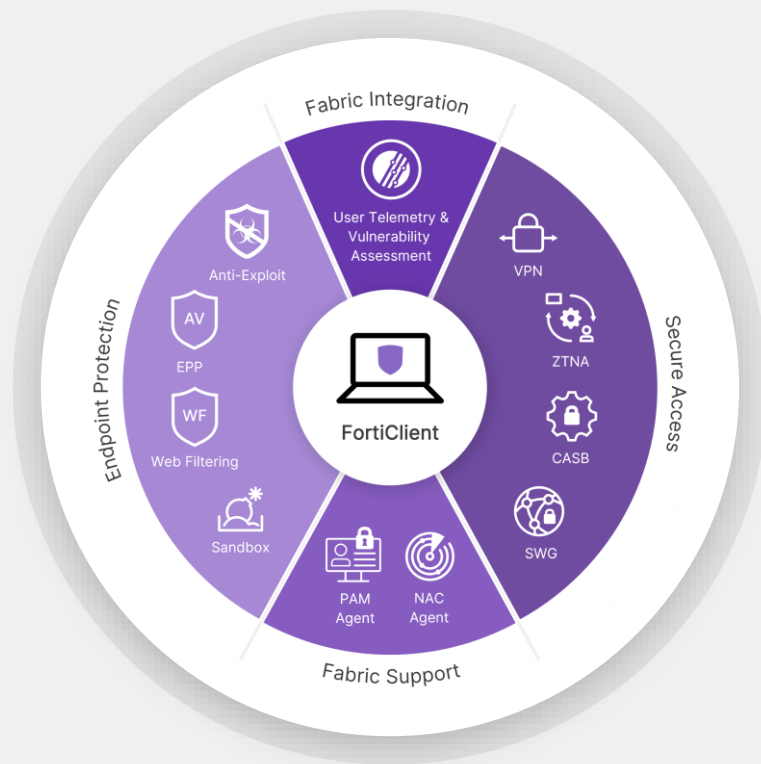
Висновки



FortiSASE



Працює як єдиний організм



Уніфікований агент

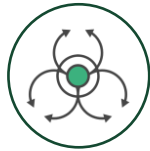


Перевірені AI сервіси та сигнатури



Ключове

Комплексний захист



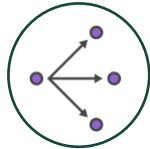
Використання AI механізмів
Безпека від Ransomware
Безпечний Інтернет

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

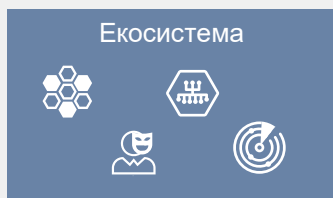
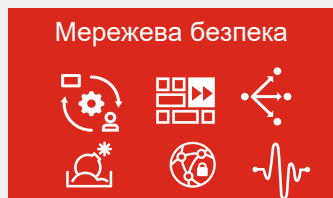
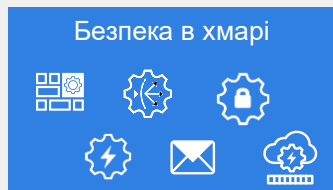
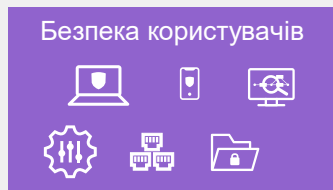
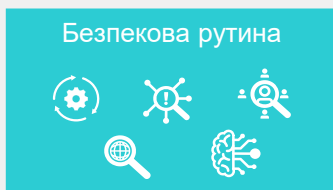
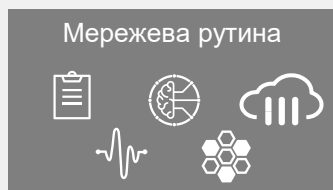
Конфіденційність даних та compliance



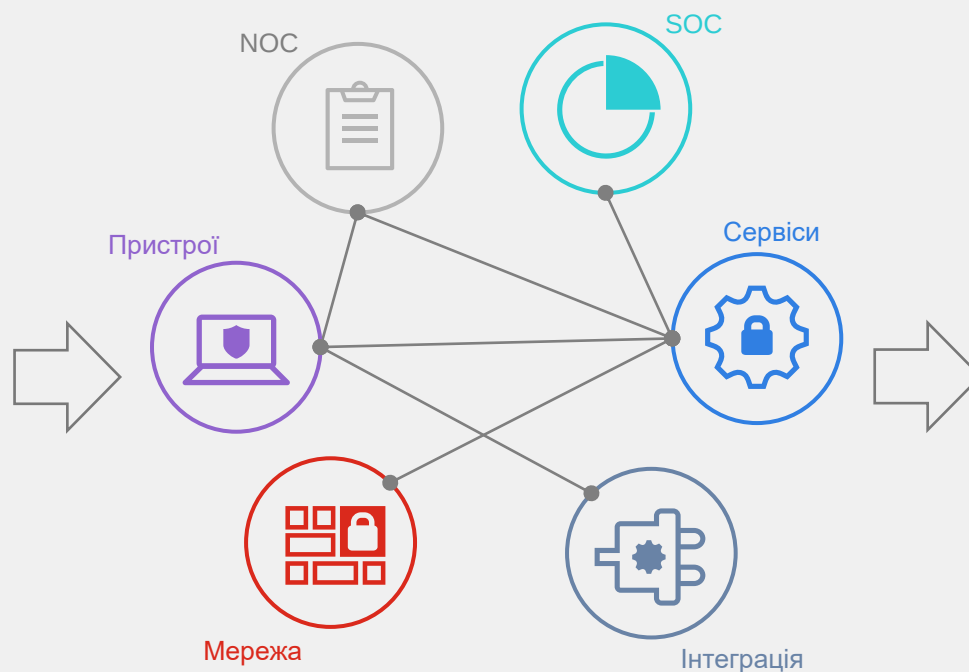
Захист критичних даних
Виконання вимог регуляторів
Захист персональної інформації

Fortinet – еволюція IT

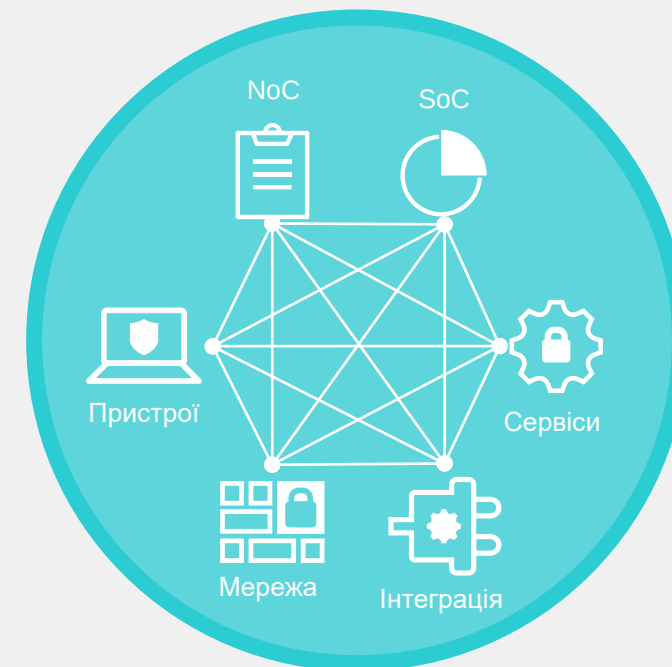
30+ виробників



10 виробників



2-3 платформи



Еволюція



Дякую за увагу!

FORTINET®