FortiEndpoint.
Уніфікований захист ПК співробітників

Євгеній Таран, Systems Engineer
ytaran@fortinet.com

Вступ

Перша довірена компанія кібербезпеки з США

Fortinet зайняв 7 місце серед компаній яким довіряє Forbes

TOP 9/10 Бізнес

TOP 10/10 Фінанси

TOP 9/10 Охорона здоров'я

TOP 10/10 Виробництво

TOP 10/10 Retail

TOP 9/10 Технологічні компанії

TOP 10/10 Телеком та оператори

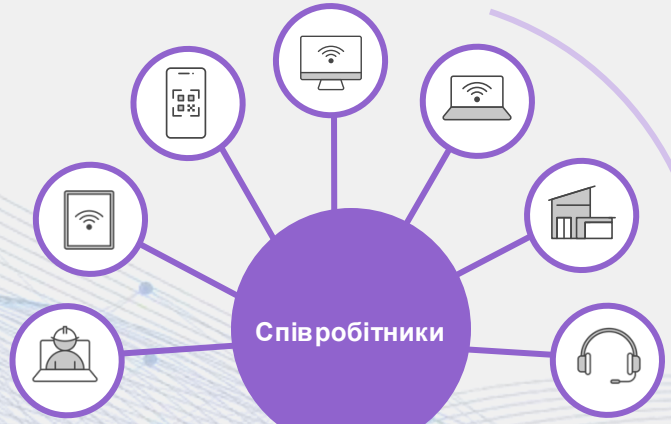
Fortinet захищає більше 805,000 компаній світу

77% з Fortune100 та **71%** Global 2000 використовуються Fortinet

Notes: Global 2000 based off 2024 Forbes list; total number of accounts is 1947 after factoring in M&A activity since publication. F100 - based off of the 2024 Fortune list; total number of accounts is 100 after factoring in M&A activity since publication.

© Fortinet Inc. All Rights Reserved.

Децентралізація та нульова довіра



84%

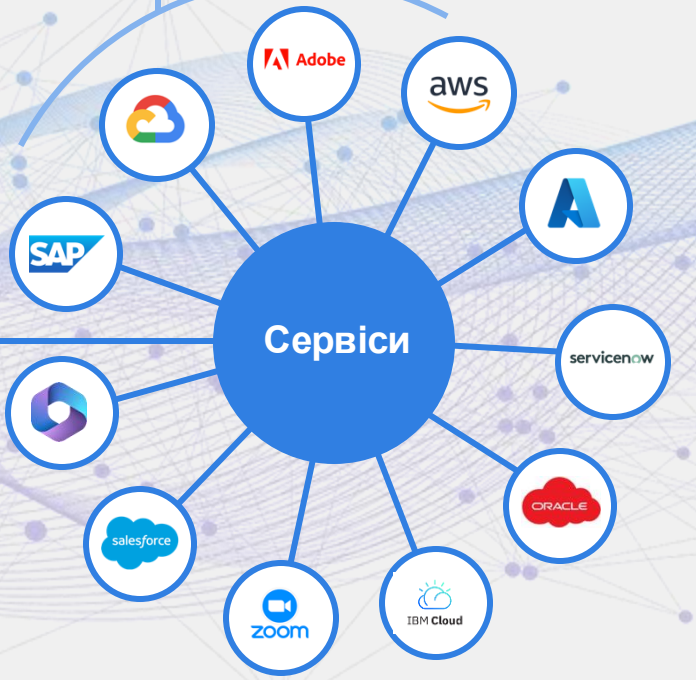
компаній гібридні

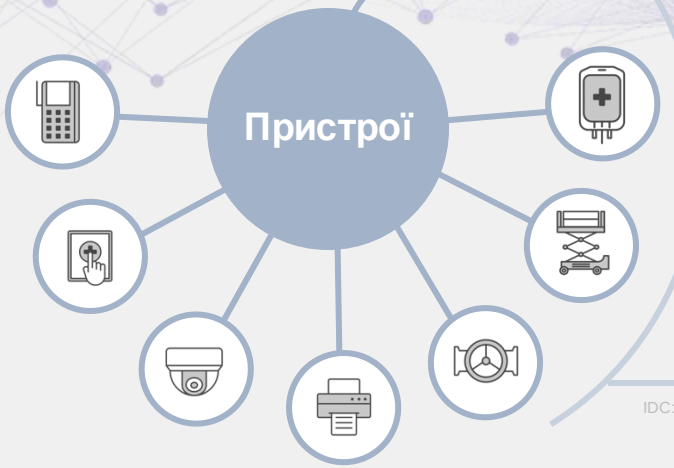
Forbes: Remote Work Statistics and Trends

125+

Різних сервісів використовуються компанією

2022 Gartner: Market Guide for SaaS Management Platforms





42 Млрд

IoT пристрої

IDC: World-Wide IDC Forecast

90%

Матимуть інциденти безпеки в філіях до 2026

2022 Gartner: 2022 Strategic Roadmap for Edge (IoT) Networking

© Fortinet Inc. All Rights Reserved.

Платформа кібербезпеки від Fortinet

Secure Networking

FortiGate
NGFW with ASIC acceleration and industry leading Convergence

FortiAP
Protected Wi-Fi connectivity via Secure Networking convergence with FortiGate

FortiNAC
Visibility, access control and automated responses for all networked devices

FortiGate Cloud
SaaS platform offering zero-touch deployment, network management and security analytics

FortiAIOps
AI based insights for rapid analysis and remediation of network issues

FortiVoice
Unified communications with secure voice, chat, conferencing, and fax

FortiRecorder
Secure NVR with smart AI analysis and centralized visibility

FGaaS
Hardware as a service for FortiGate

FortiSwitch
Protected Ethernet connectivity via Secure Networking convergence with FortiGate

FortiManager
Centralized management of your Fortinet security infrastructure

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

FortiEdge Cloud
Cloud management for standalone LAN, WLAN and 5G gateway equipment

FortiFone
Robust IP phones and softclient to stay connected from anywhere

FortiCamera
Physical security with intelligent motion detection in any light condition

FortiConverter
Secure and automated firewall migration from a broad spectrum of vendors

Resources

Product Matrix
Specifications for top selling models

Free Training
Fortinet is committed to training over 1 million people by 2025

FortiOS
The Heart of the Fortinet Security Fabric

Fortinet Brochure
Highlighting our broad, integrated, and automated solutions, quarterly

Free Assessment
Perform an assessment in your network to validate your existing controls

FortiCare
Support and mitigation services

Unified SASE

SASE

FortiGate SD-WAN
Application-centric, scalable, and Secure SD-WAN with NGFW

FortiClient ZTA Agent
Remote access, application access, and risk reduction

FortiProxy
Enforce internet compliance and granular application control

FortiCASB
Prevent misconfigurations of SaaS apps and meet compliance

FortiClient EPP Agent
Endpoint Protection Agent with AV, URL and Sand-box

FortiSASE
Cloud-delivered Security Services Edge

FortiMonitor
SaaS based DEM platform, performance monitoring

FortiEndpoint
XDR, ZTNA and EPP as unified agent

CLOUD

FortiGate VM
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiWeb
Prevent web application attacks against critical web assets

FortiGSLB
Ensure business continuity during unexpected network downtime

FortiFlex
Flexible daily usage-based consumption licensing for a broad catalog of solution

FortiGate CNF
Hosted cloud-native firewall for simplified cloud network security

FortiADC
Application-aware intelligence for distribution of application traffic

FortiDDoS
Machine-learning quickly inspects traffic at layers 3, 4, and 7

FortiPoints
Simplified, flexible licensing for annual contracts, renewals, upgrades, and co-terms

AI-Powered FortiGuard Security

- Web Filtering
- IPS
- AV
- Sandbox
- IL MPS
- Application Control
- Attack Surface
- DLP
- OT Security Services
- IoC
- IL CASB

Security Operations

FortiAnalyzer
Security Fabric log management, monitoring and response

FortiSIEM
Enterprise-wide monitoring, threat detection, and response

FortiEDR/XDR
Automated endpoint protection and correlated incident response

FortiSOAR
Automated security operations, investigation, and response

FortiNDR
AI-driven analysis to detect and respond to threats

SOCaaS
Continuous security monitoring, incident triage, and escalation

IR Services
Rapid detection, containment, and recovery of cyberattacks

FortiDeceptor
Active deception platform for early in-network attack detection and response

FortiTrust Identity
Identity and Access Management as a Service (IDaaS)

FortiGuest
Access management solution for temporary access to guests and visitors

FortiCNAPP
Secure code to cloud with a single, data-driven platform

FortiNextDLP
Endpoint DLP and Insider Risk management

FortiMail
AI-powered, protection against email-borne threats

FortiSandbox
AI-powered real-time protection against unknown and 0-day threats

FortiToken
Cloud/HW/Mobile MFA provide passwordless adaptive authentication

FortiAuthenticator
Centralized identity and access management solution

FortiGuard MDR Service
Managed threat detection, investigation, and response

FortiRecon
Proactive digital risk protection service and external/internal threat monitoring

FortiPAM
Privileged identity and access management, and session monitoring

FortiTester
Network performance testing and breach attack simulation (BAS)

FortiDevSec
Orchestrated and automated continuous application security testing

FortiDAST
Automated black-box dynamic application security testing

FortiScanner Cloud
Cyber Asset Attack Surface Management Service

FortiAI
Integrated GenAI Assist for SOC and NOC

OT Security Platform

OT Security Service
FortiGuard subscription for FortiGate NGFW enables protection against OT-specific threats

Ruggedized Products
Rugged NGFW, switch, AP, and 5G extenders provide secure connectivity in harsh outdoor environments

FortiSRA
Agentless secure remote access offers robust remote access control, management, session logging, monitoring, and recording

SecOps for OT
Advanced cybersecurity controls bring OT networks into the SOC and incident response plans

Open Ecosystem

FNDN
Advanced tools for Fortinet community to develop custom solutions

Fabric Connectors
Fortinet-developed integrations for automation and security

Fabric API
Partner-developed integrations for end-to-end visibility and protection

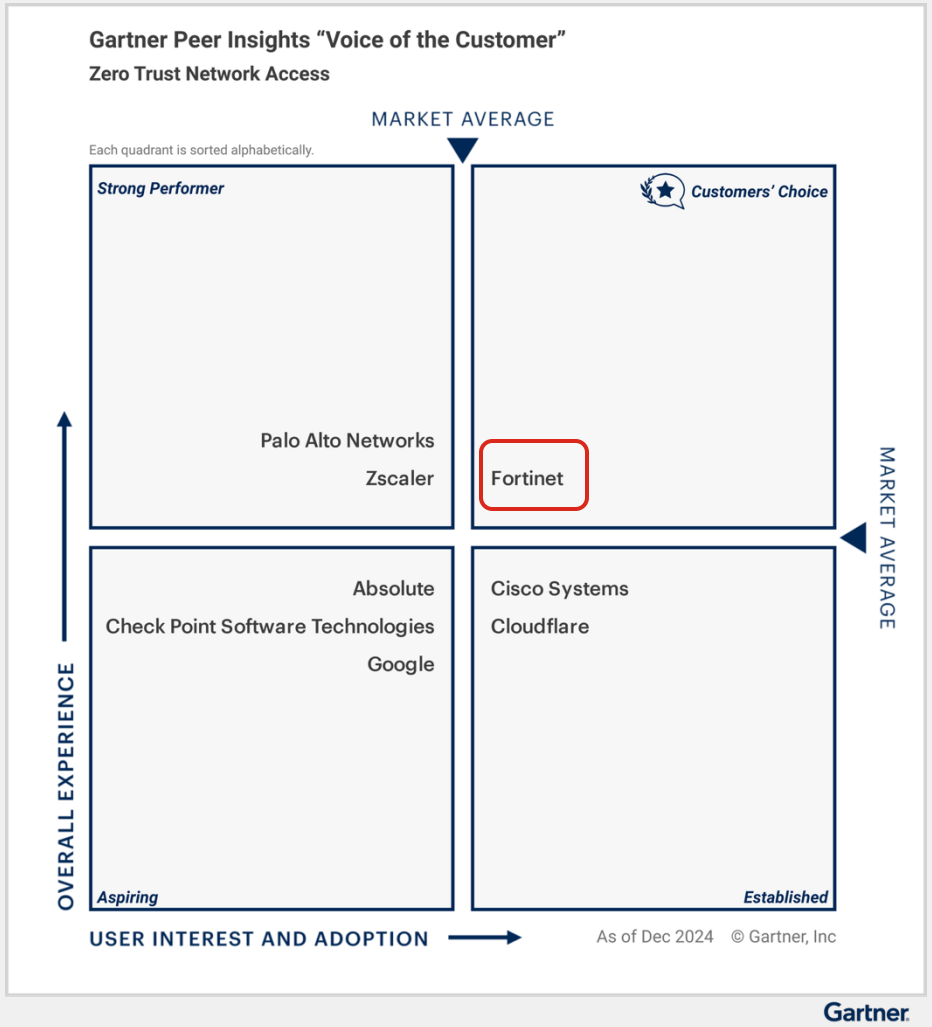
DevOps Tools
Community-driven scripts automate network/security tasks

Extended Ecosystem
Integrates with third-party systems and orgs for sharing threat-intel

© Fortinet Inc. All Rights Reserved.

2025 Gartner Peer Insights ZTNA

Fortinet став вибором користувачів в 2025 Gartner Peer Insights



“Це був дивовижний досвід роботи з Universal ZTNA Fortinet. Ми користуємося цим продуктом протягом останніх 2-3 років. Ми не стикалися з жодними збоями, підключення користувачів безперебійне. Fortinet Universal ZTNA забезпечує стабільну безпеку для всіх користувачів, незалежно від того, чи вони локальні чи в роумінгу, запроваджуючи однакову політику в усій організації.»

Рецензент: Мережі та безпека індустрії телекомунікацій.

“Я використовую Fortinet Universal ZTNA і він чудово підходить для безпеки мережі. Він захищає як віддалених, так і локальних користувачів, забезпечуючи лише авторизований доступ. Легка інтеграція з іншими продуктами Fortinet робить керування легким. Налаштування просте, а інтуїтивно зрозумілий інтерфейс робить його зручним для користувача. Рекомендую його як надійне ZTNA рішення.”

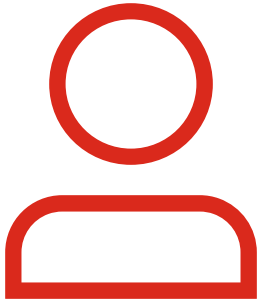
Рецензент : IT Менеджер індустрії споживчих товарів

© Fortinet Inc. All Rights Reserved.

З чого починається ZTNA

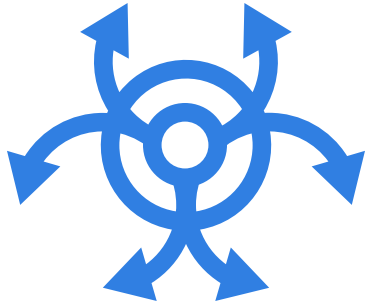
BYOD та віддалена робота стала буденність

Робота звідусіль



- Збільшення векторів атак
- Вразливості ПК

Цільові атаки



- Профільні угрупування
- Проникнення та розповсюдження

Хмарні та SaaS сервіси

- Захист інформації
- Моніторинг

© Fortinet Inc. All Rights Reserved.

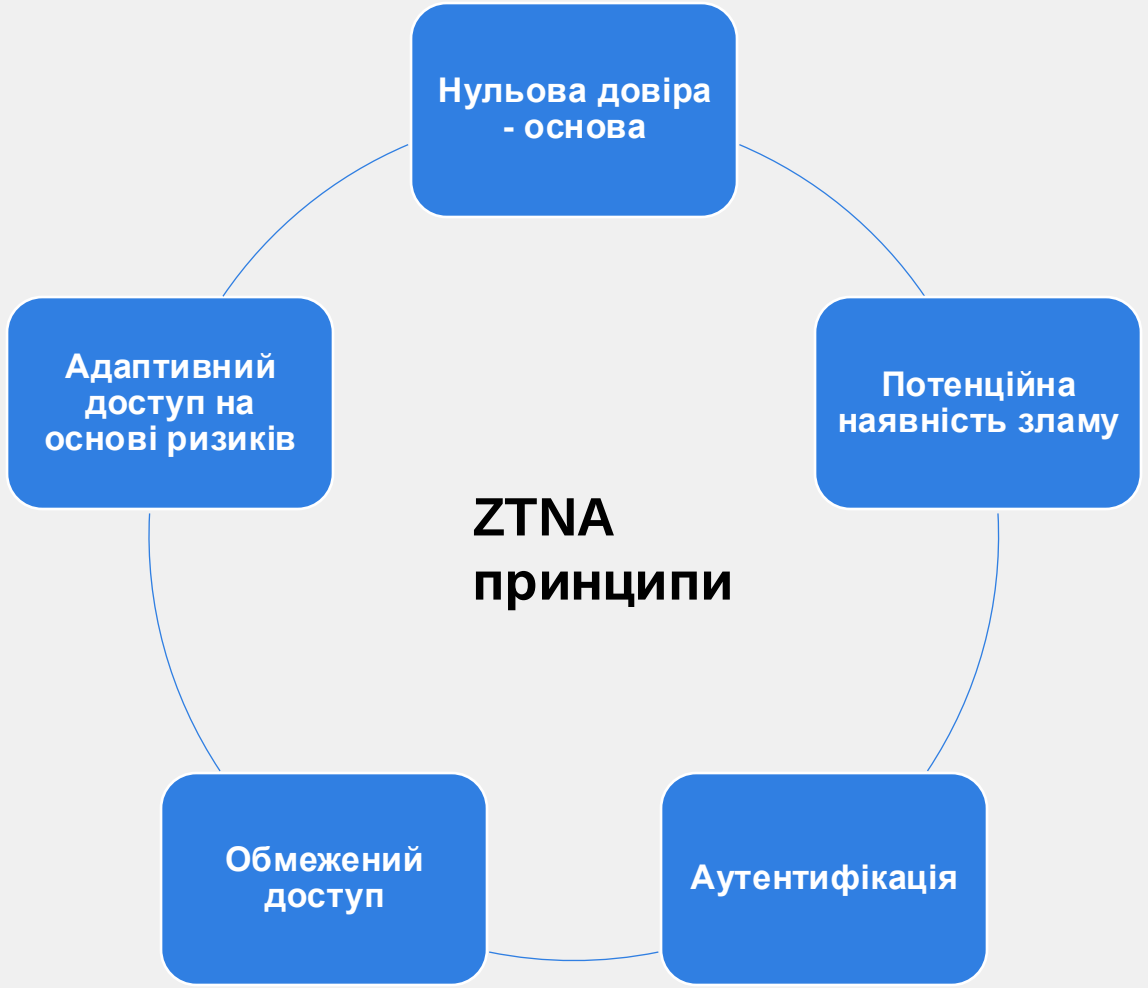
ZTNA принципи

Ніколи не довіряй. Завжди перевіряй.

Надає доступ до мережі лише після автентифікації та авторизації особи

Обмежує доступ до мережі лише необхідними ресурсами/додатками

Контролює доступ до мережі майже в режимі реального часу залежно від контексту пристрою/користувача



Джерело: Gartner

© Fortinet Inc. All Rights Reserved.

Еволюція віддаленого доступу з ZTNA

Старий віддалений доступ

Базовий

Широкий доступ
(Ignores least-privilege access)

Разова верифікація
(User Identity check with or without MFA)

Відсутня безпекова інспекція та захист даних

Статичний контроль доступу

Різні платформи для хмари та ДЦ

ZTNA

Наступний крок

Тонкий доступ до сервісів
(least-privilege explicit application access)

Постійна верифікація
(Користувач/пристрій та стан пристрою)

Глибока інспекція та захист даних

Адаптивний доступ враховуючи ризики

Один продукт покриває ДЦ та SaaS

© Fortinet Inc. All Rights Reserved.

Перші кроки

3 чого зазвичай починають?

Основа

NGFW

FortiOS

FortiOS виконує перевірку доступу, підтримує таблицю доступу до груп користувачів/додатків, проксі-додатків
(FOS 7.0+)

ZTNA та безпековий агент

FortiClient/Central Management

FortiClient EMS
FortiClient ZTNA agent
(FortiClient 7.0+)

Опція

Другий фактор

FortiAuthenticator

FortiToken

FortiTrust Identity

та сторонні ID провайдери в рамках Security Fabric

© Fortinet Inc. All Rights Reserved.

Для кого?

Офісні співробітники нарівні з віддаленими

Перевірка кожної сесії

Перевірка користувача

- Кілька факторів
- Пароль
- SSO
- Робочий час

Перевірка пристрою

- Інформація щодо пристрою
- Версія ОС
- Інформація щодо антивіруса
- Сканер вразливостей

Постійна перевірка

- Статус пристрою
- Дії користувача
- Вразливості

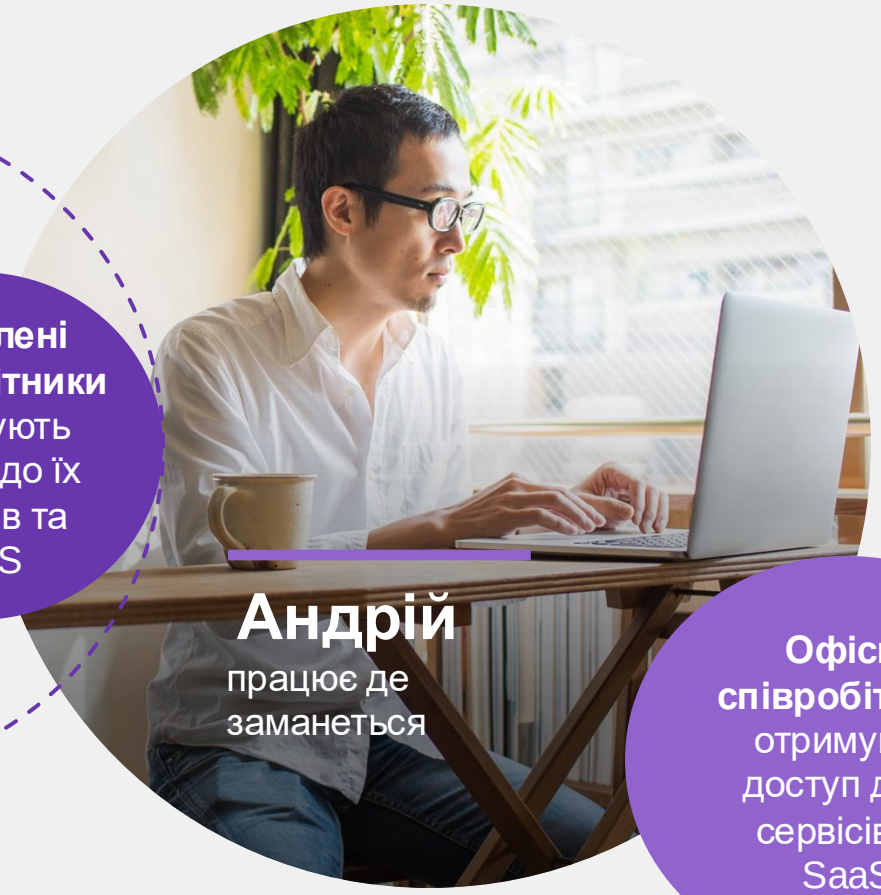
Детальний контроль

Доступ тільки до потрібних сервісів

© Fortinet Inc. All Rights Reserved.

Для кого?

І як це працює

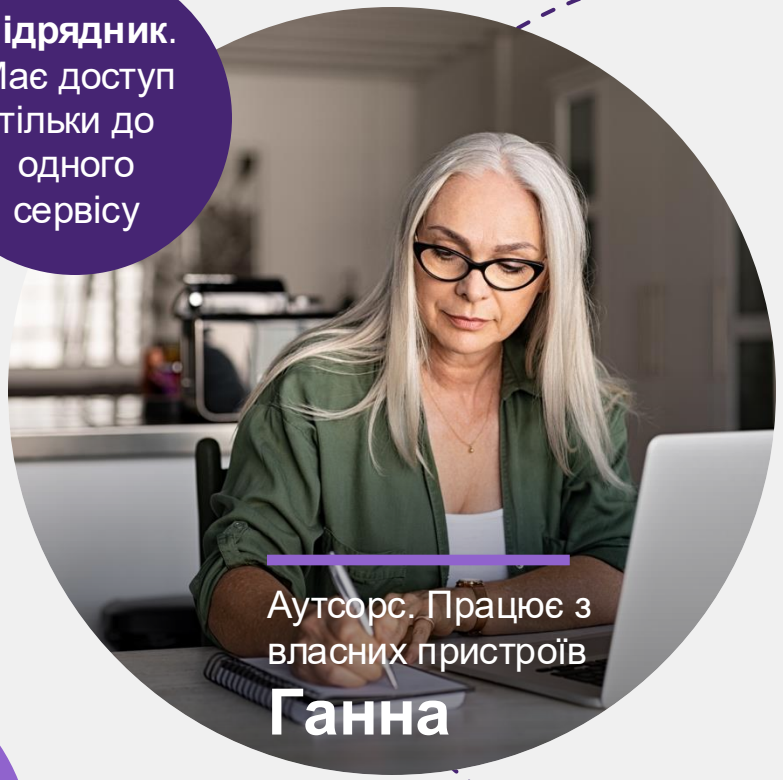


Віддалені співробітники отримують доступ до їх сервісів та SaaS

Андрій
працює де заманеться

Офісні співробітники отримують доступ до їх сервісів та SaaS

Підрядник. Має доступ тільки до одного сервісу



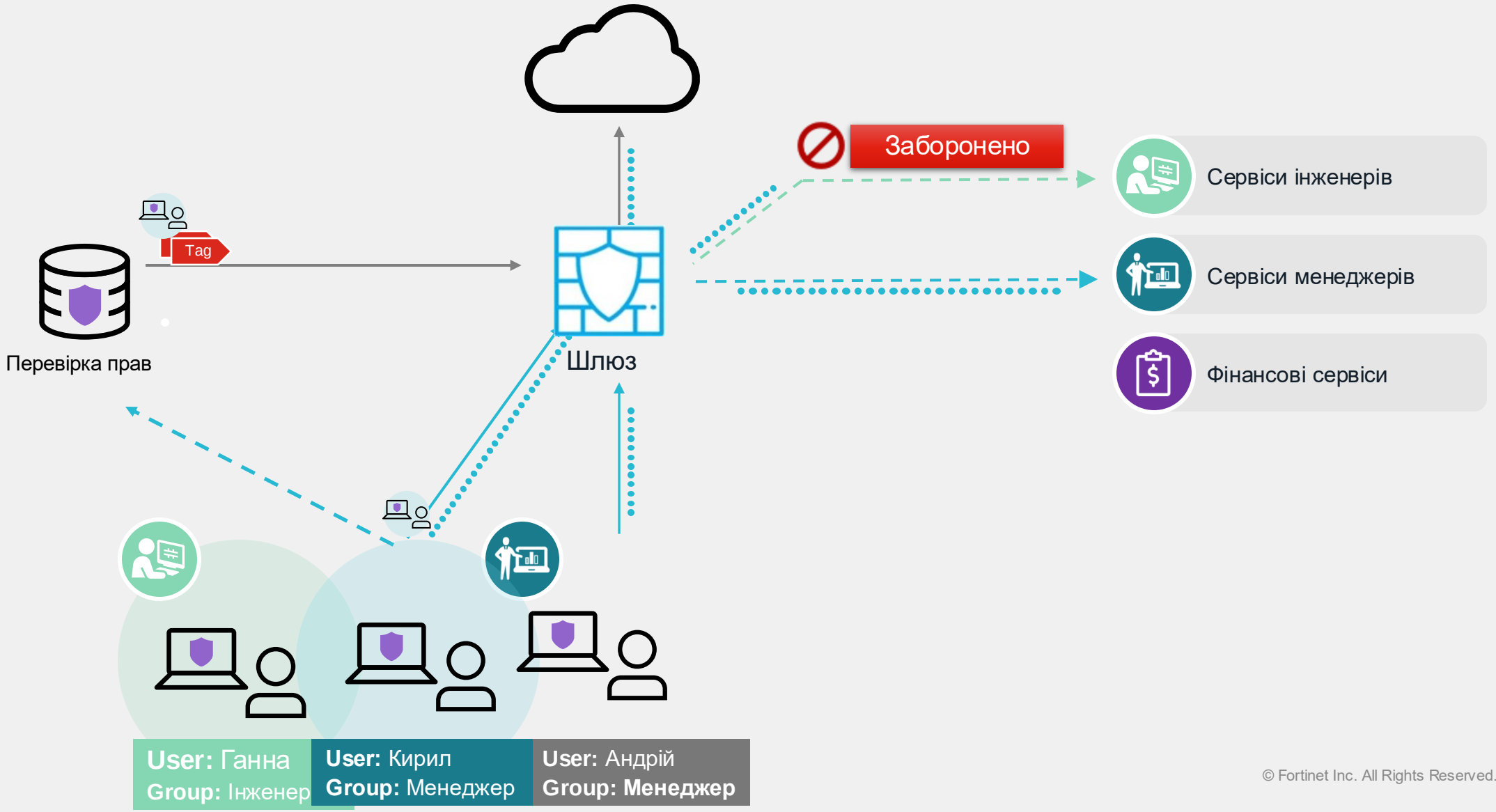
Аутсорс. Працює з власних пристроїв

Ганна

© Fortinet Inc. All Rights Reserved.

Розподілення доступу

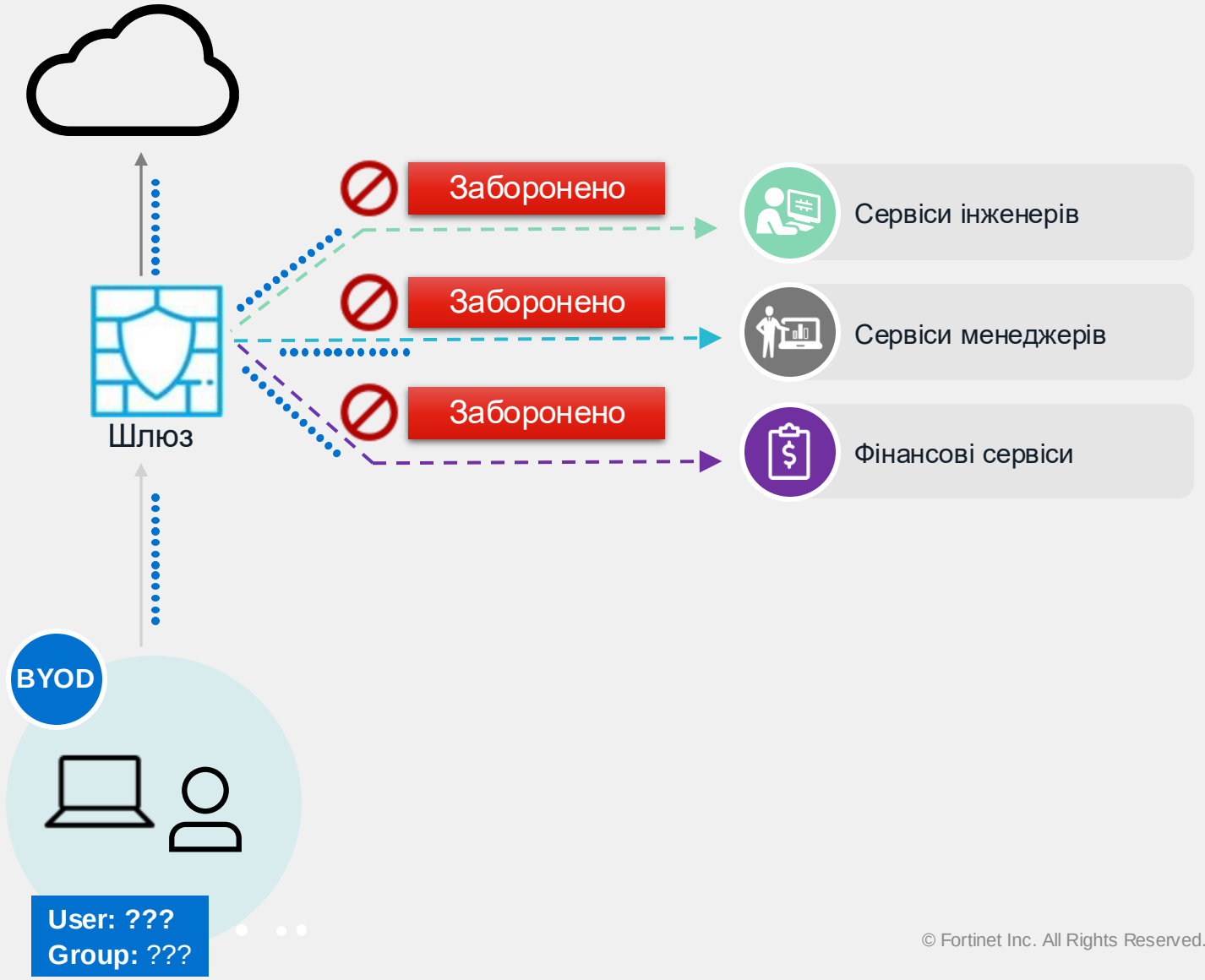
На основі прав



© Fortinet Inc. All Rights Reserved.

Робота з іншого ПК

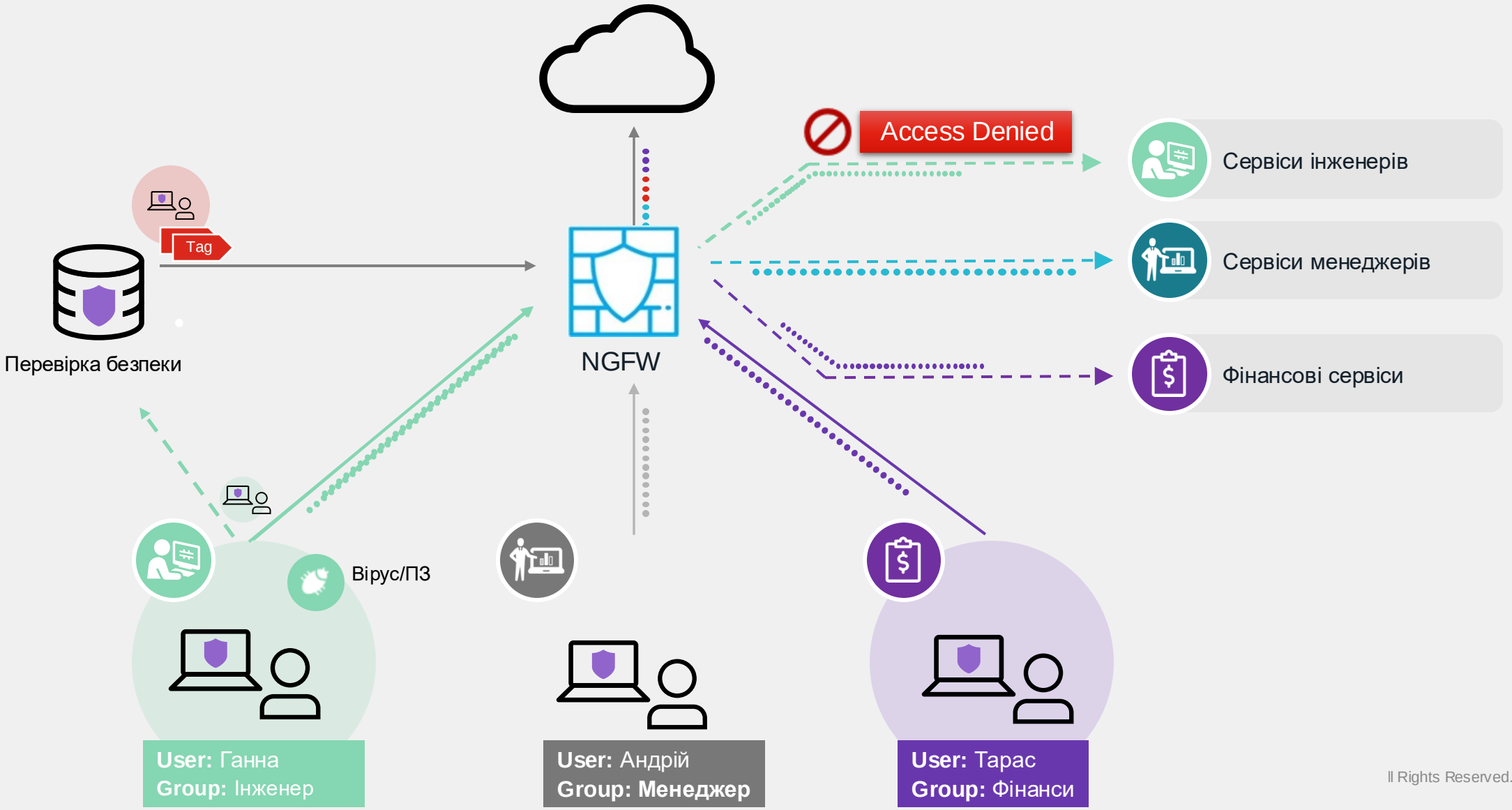
Неперевірений ПК



© Fortinet Inc. All Rights Reserved.

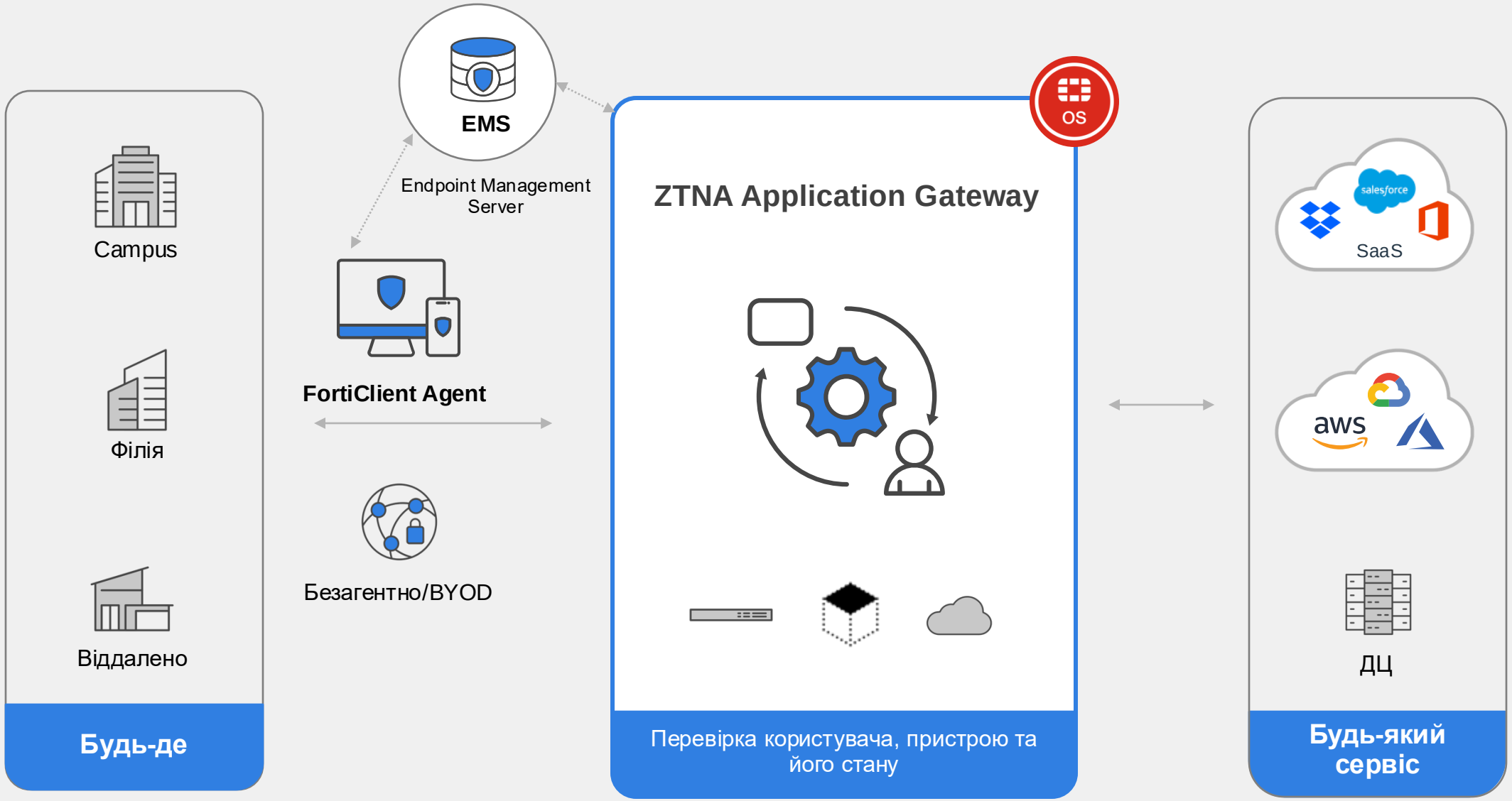
Блокування зараженого пристрою

Або коли користувач «підхопив вірус»



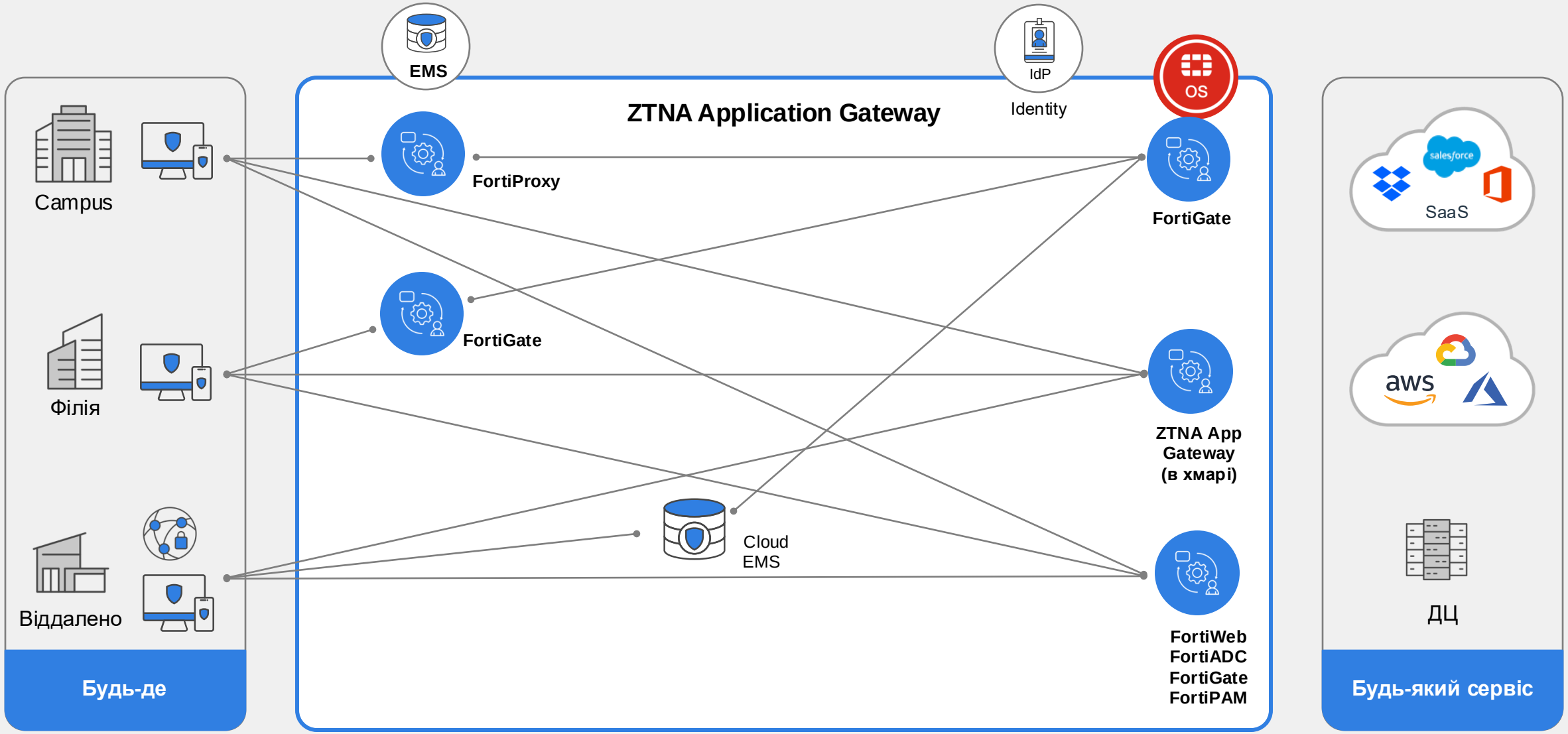
ll Rights Reserved.

Універсальне ZTNA рішення



© Fortinet Inc. All Rights Reserved.

Універсальне ZTNA рішення



© Fortinet Inc. All Rights Reserved.

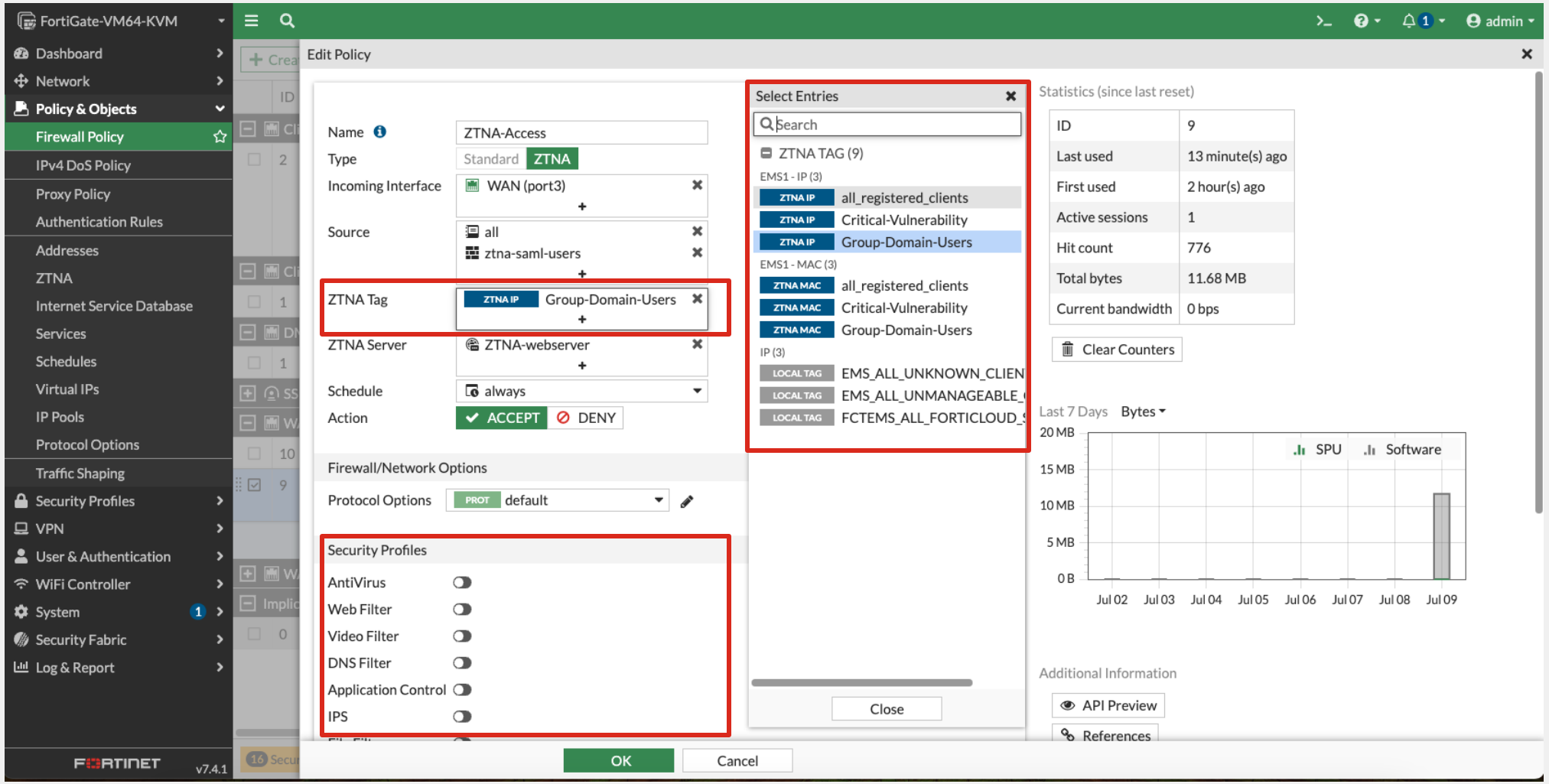
Еволюція ZTNA

ZTNA	Універсальний ZTNA

© Fortinet Inc. All Rights Reserved.

Перевод політик на ZTNA Tags

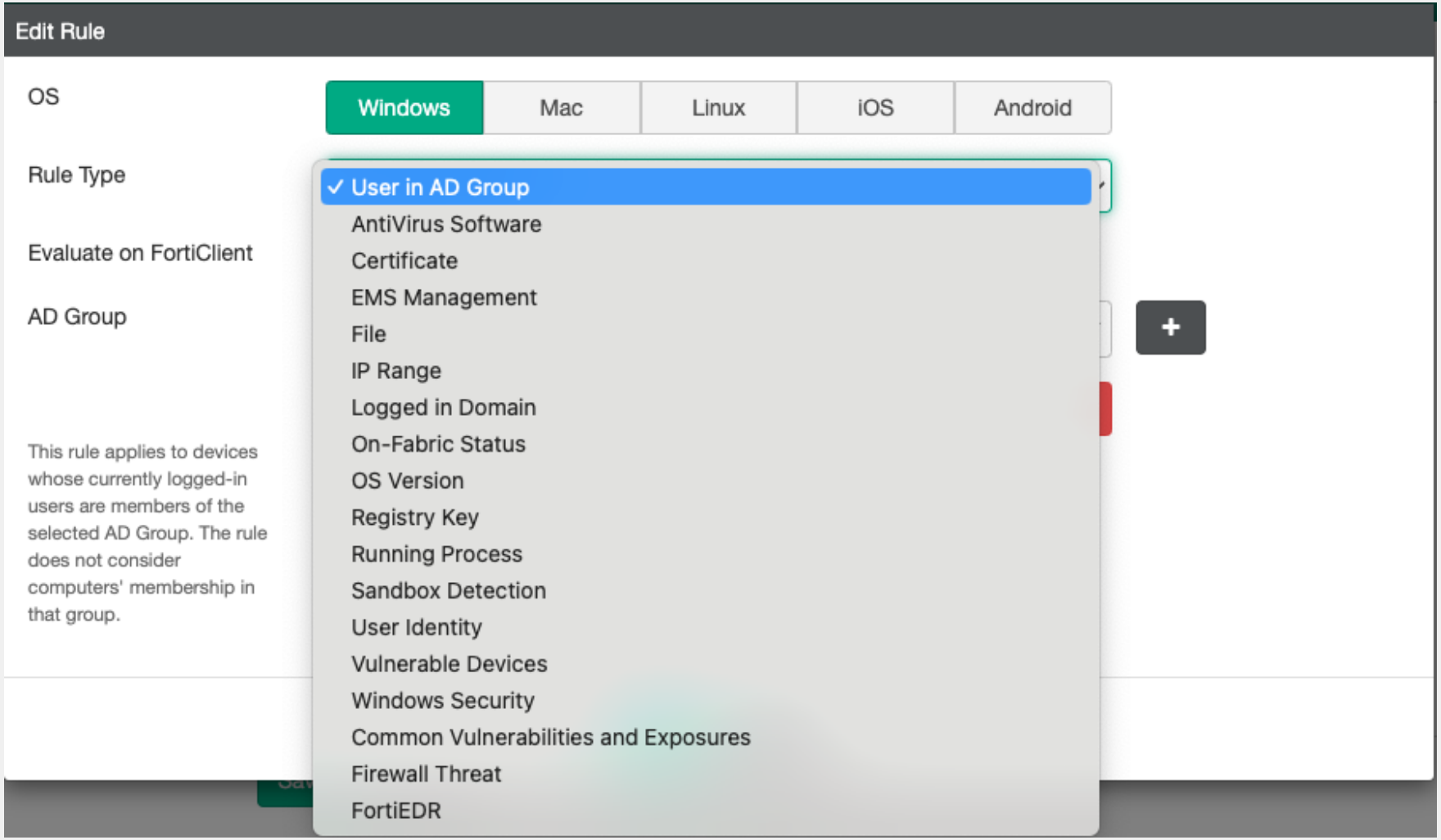
Етап 1



- Оберіть один або кілька ZTNA tags
- З підтримкою безпеки

© Fortinet Inc. All Rights Reserved.

Вибір правил перевірки на основі одного чи кількох критеріїв



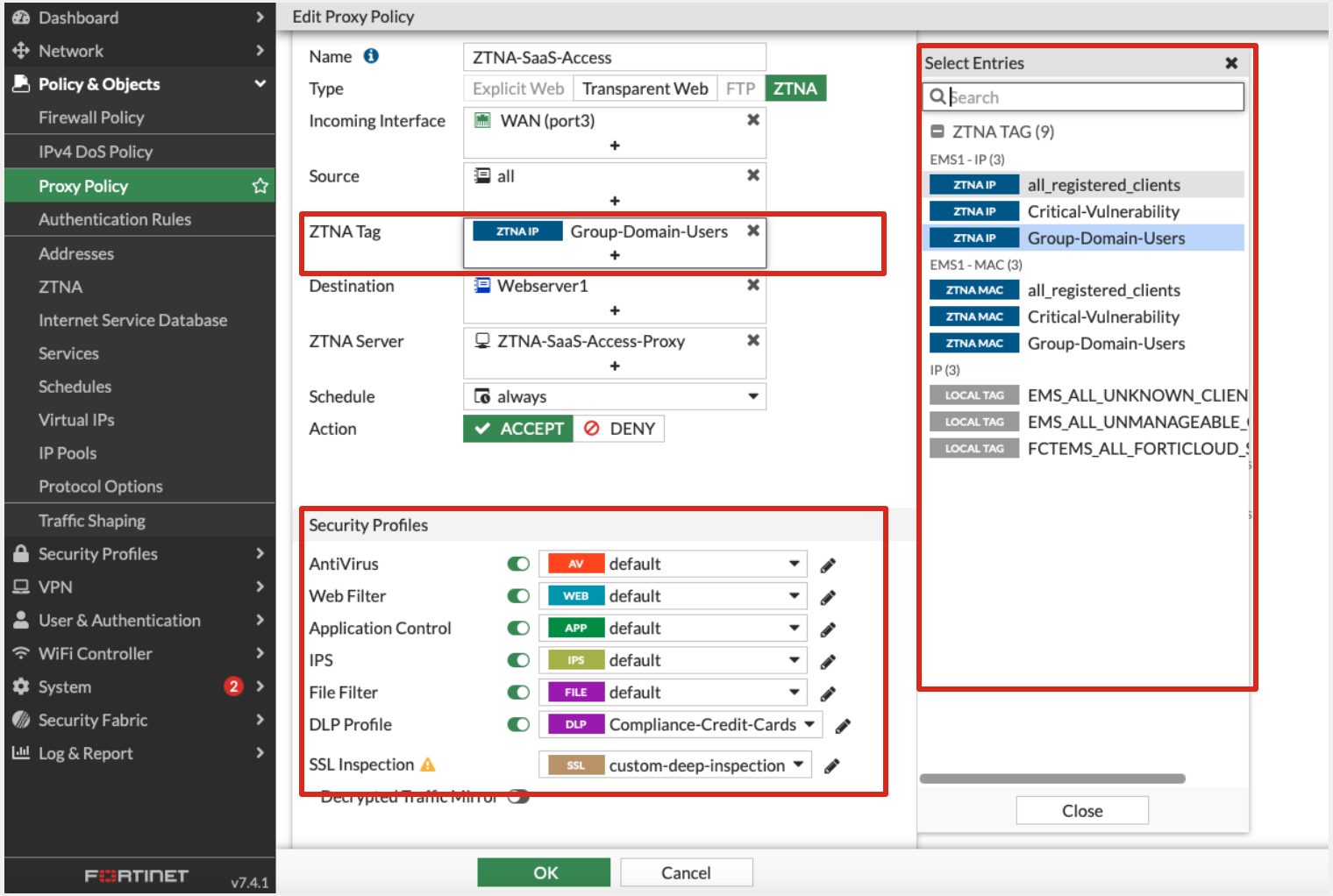
Zero Trust Tags

- User AD group, Domain
- Security Software (e.g., AV)
- Vulnerability Status, CVE
- OS, Registry Key, Process
- On-net/Off-net, Identity, IP

© Fortinet Inc. All Rights Reserved.

Перевірка трафіку

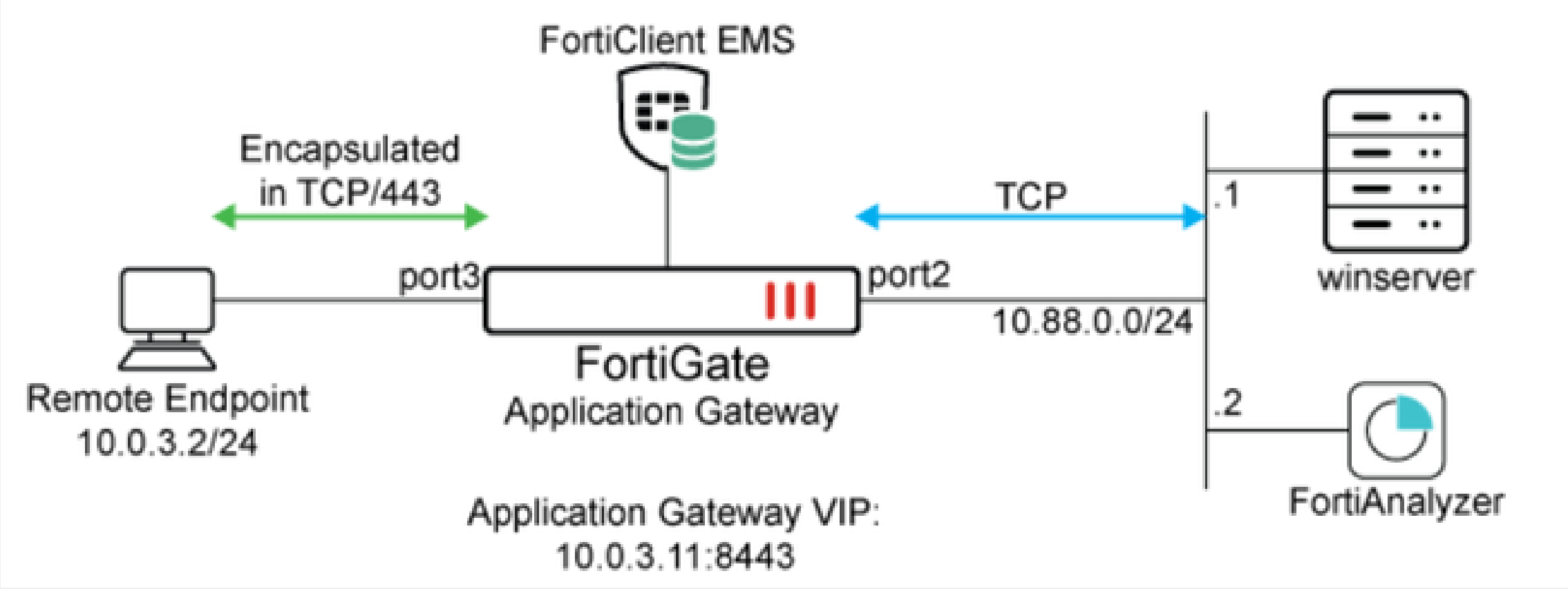
Етап 2



- Поступове увімкнення безпеки
- В першу чергу критичні сервіси

© Fortinet Inc. All Rights Reserved.

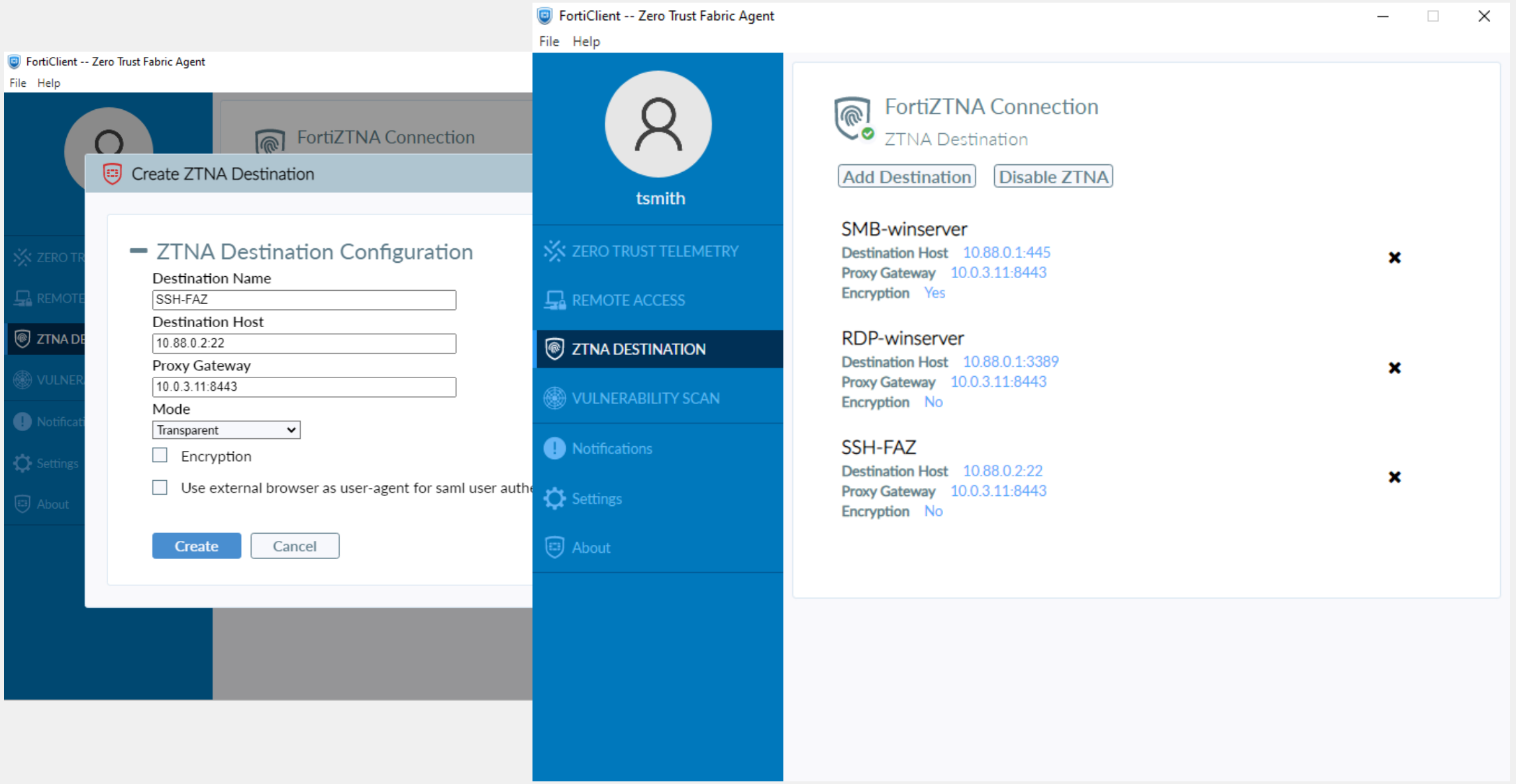
Доступ без VPN (ZTNA destination)



https://community.fortinet.com/t5/FortiClient/Technical-Tip-How-to-implement-ZTNA-Destination-in-FortiClient/ta-p/318880

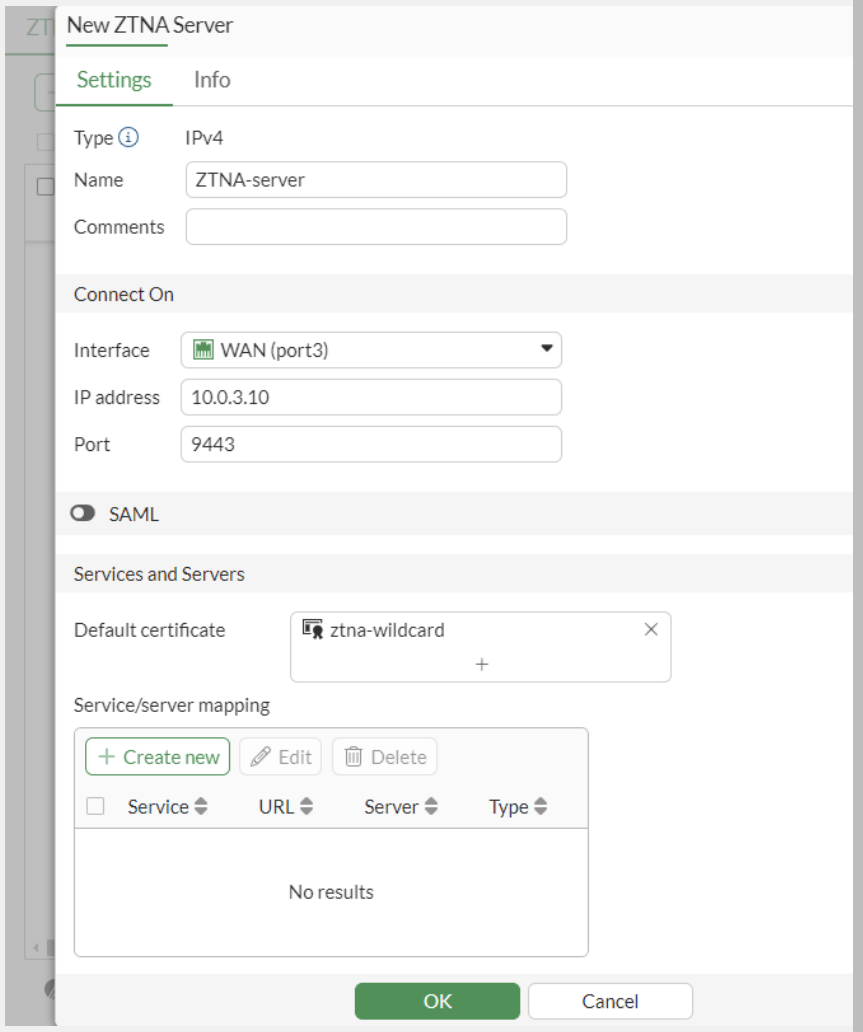
© Fortinet Inc. All Rights Reserved.

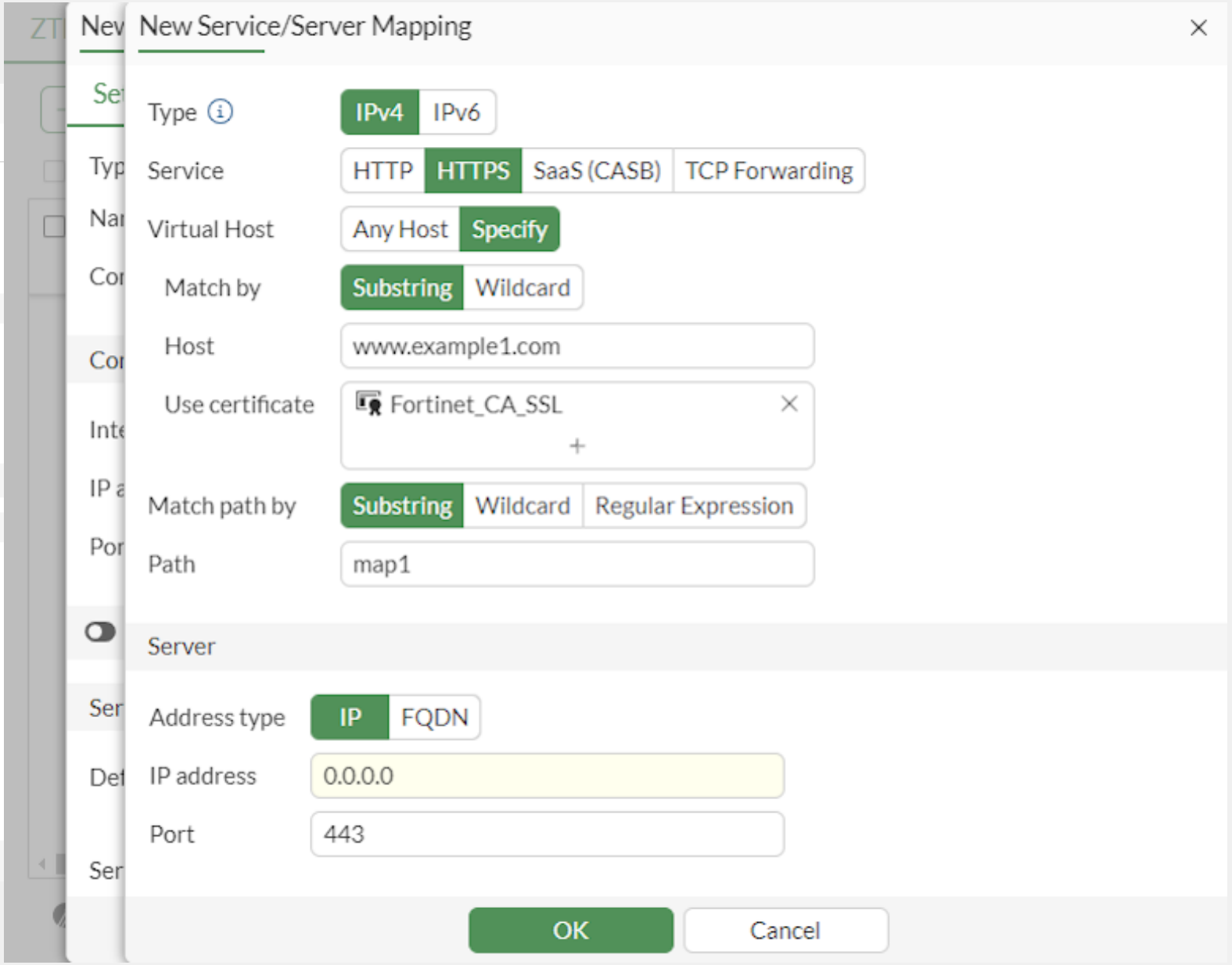
Доступ без VPN (ZTNA destination)



© Fortinet Inc. All Rights Reserved.

Доступ без VPN
ZTNA destination

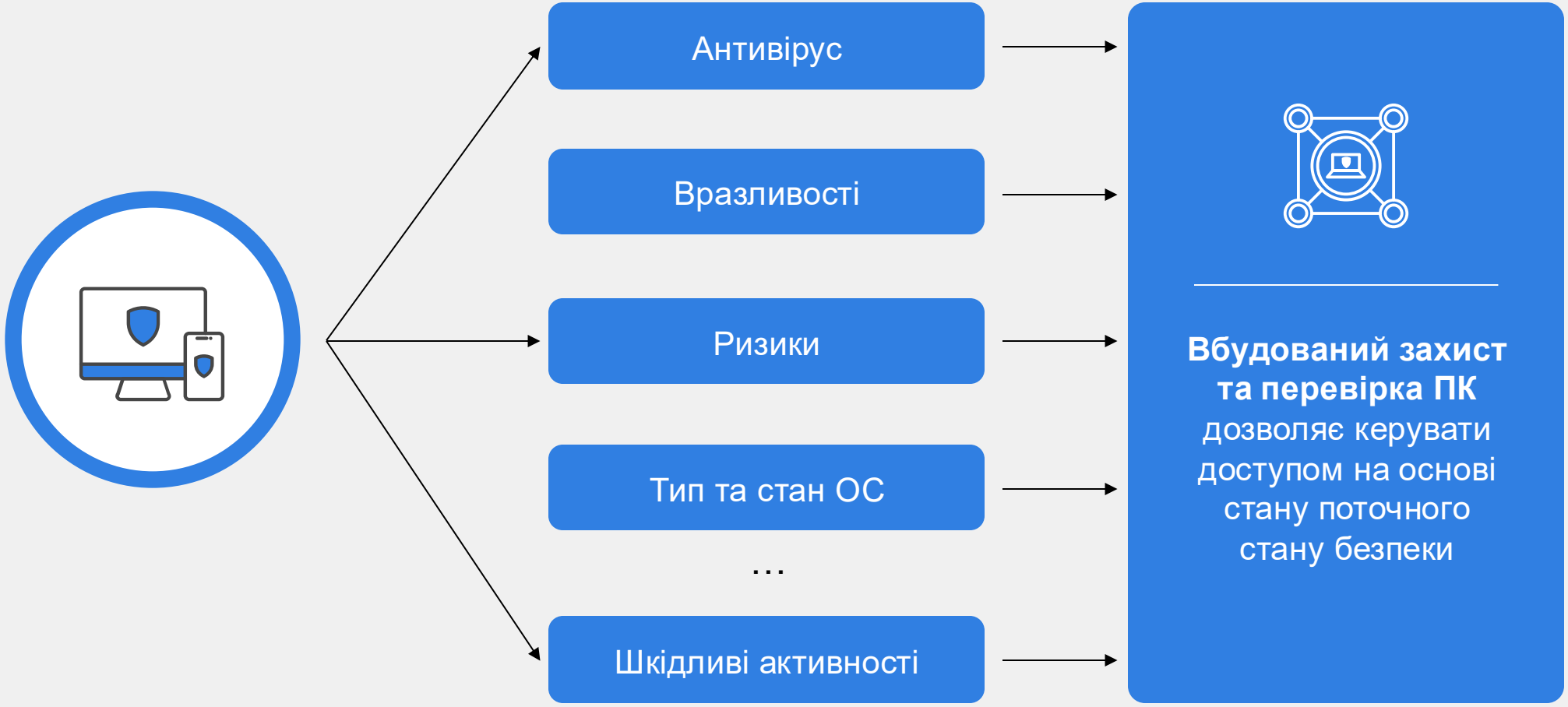




© Fortinet Inc. All Rights Reserved.

Інтегрована безпека що приймає участь в ZTNA

Постійна перевірка пристрою



© Fortinet Inc. All Rights Reserved.

Vulnerability Name	FortiGuard ID	CVE ID	Category	Affected Endpoints	Patch Type
Cumulative Security Update for Internet Explorer	1492	CVE-2016-0178	OS	3	Patch
Firefox SVG Animation Remote Code Execution	31801	CVE-2016-9079	Browser	3	Patch
Sandbox restrictions not applied to nested frame elements	26051	CVE-2016-3223	AntiVirus	2	Patch
Security update available for Adobe Reader APSB17-01	38632	CVE-2017-2939	OS	2	Scheduled
Security Update for Group Policy					Scheduled
Security Update for Microsoft Graphics Component					Scheduled
Security Update for Microsoft RPC					Scheduled
Security Update for Microsoft Windows to Address Remote Code Executio					Scheduled
Security Update for Microsoft XML Core Services					Scheduled
Security Update for Netlogon					Scheduled
Security Update for Windows Print Spooler Components					Scheduled
Security Update for Windows Shell					Scheduled
Security Updates Available for Adobe Acrobat and Reader APSB16-09					Scheduled
Security Update for Adobe Flash Player					Scheduled
Security Vulnerability CVE-2016-5183 for Google Chrome					Scheduled
Security Vulnerability CVE-2016-5182 for Google Chrome					Scheduled
UI selection timeout missing on download prompts	26255	CVE-2016-0146	AntiVirus	1	Scheduled
Use after free mutating DOM during SetBody	22566	CVE-2016-0139	AntiVirus	1	Scheduled
WebGL content injection from one domain to rendering in another	27578	CVE-2016-0274	AntiVirus	1	Scheduled

Affected Endpoints

Hostname	User	Last Seen	Scan Time
AHarris-PC	Andrew	2017-02-05 12:32:21	2017-02-05 12:32:21
km-ftnt-PC	admin	2017-02-04 18:25:45	2017-02-04 18:25:45
TiaraQuan-PC	Administrator	2017-02-04 09:15:22	2017-02-04 09:15:22

OK

FortiGuard Web Filtering

Аналіз за допомогою штучного інтелекту

- Контрольовані та самостійні моделі
- Навчання на базі даних FortiGuard Labs

Консистентні дані

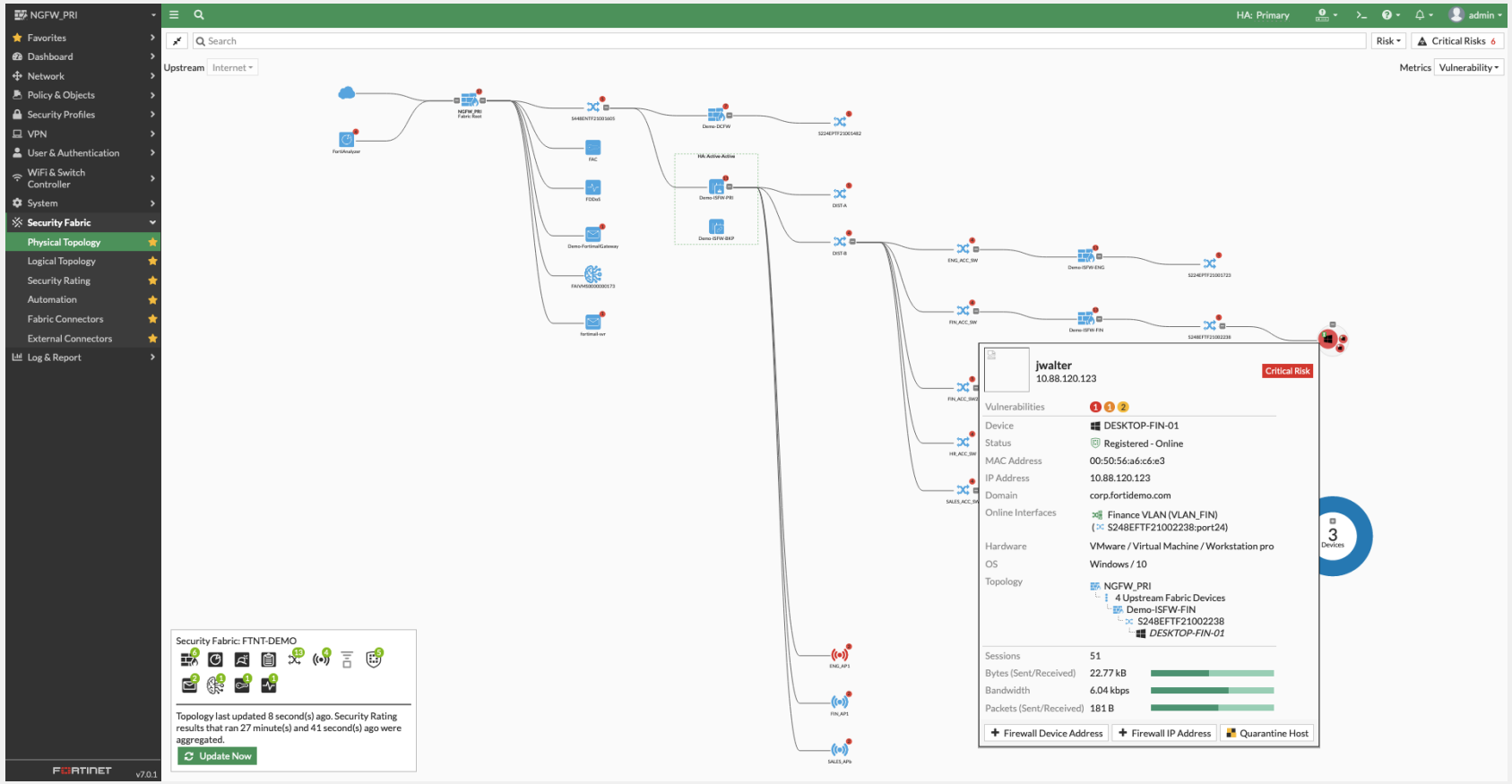
- Мережеві пристрої, ПК та хмари
- Різні можливості розгортання

Захист в деталях

- Повний спектр веб-захисту від невідомих і відомих загроз
- Кілька рівнів захисту з майже нульовими помилковими результатами

© Fortinet Inc. All Rights Reserved.

Деталізація до рівня пристрою та користувача



- Інформація про пристрій
  - OS
  - MAC
- Статус FortiClient
- Вразливості ПК
- Користувач
- Аватар користувача
- Соціальні мережі
- Online/Off-line
- Події та журнали

© Fortinet Inc. All Rights Reserved.

Впровадження ZTNA

Етап 1

- VPN з перевіркою ПК
- Перевірка **до** VPN підключення
- Постійна перевірка під час підключення

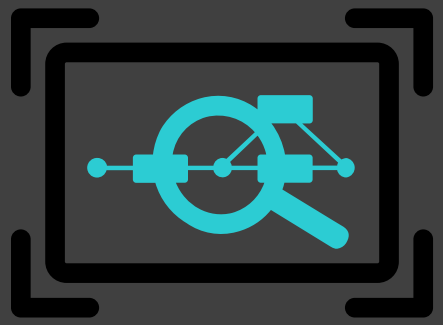
Етап 2

- ZTNA для кожного сервісу
- Особливі перевірки для ТОП сервісів (ERP, файл-сервер)
- Розширена постійна перевірка ПК

Етап 3

- Розширення ZTNA на всі сервіси
- Інтеграція з EDR одним агентом

© Fortinet Inc. All Rights Reserved.

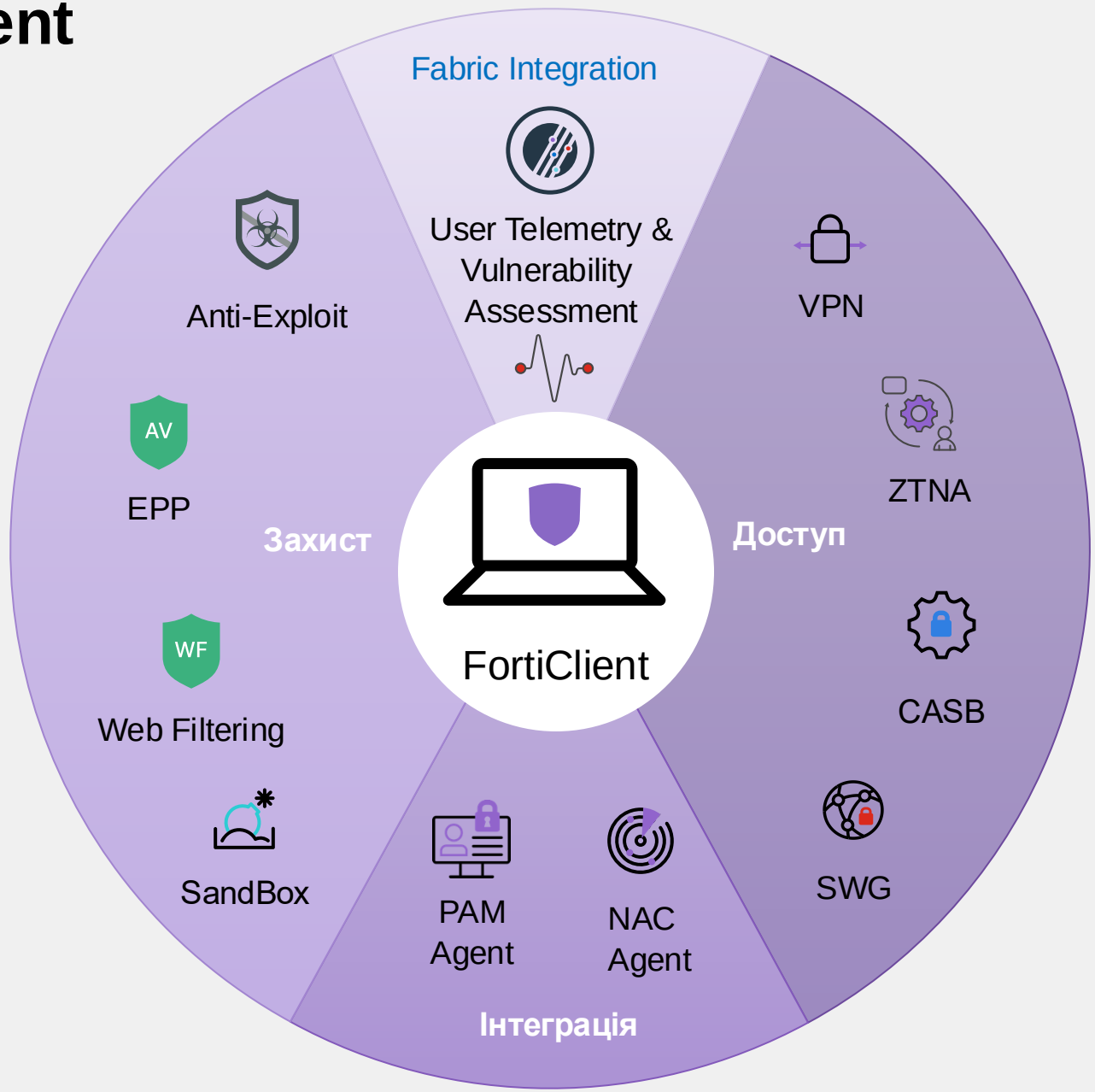


З чого починається EDR/XDR

Уніфікований агент - FortiClient

Один агент для всього*

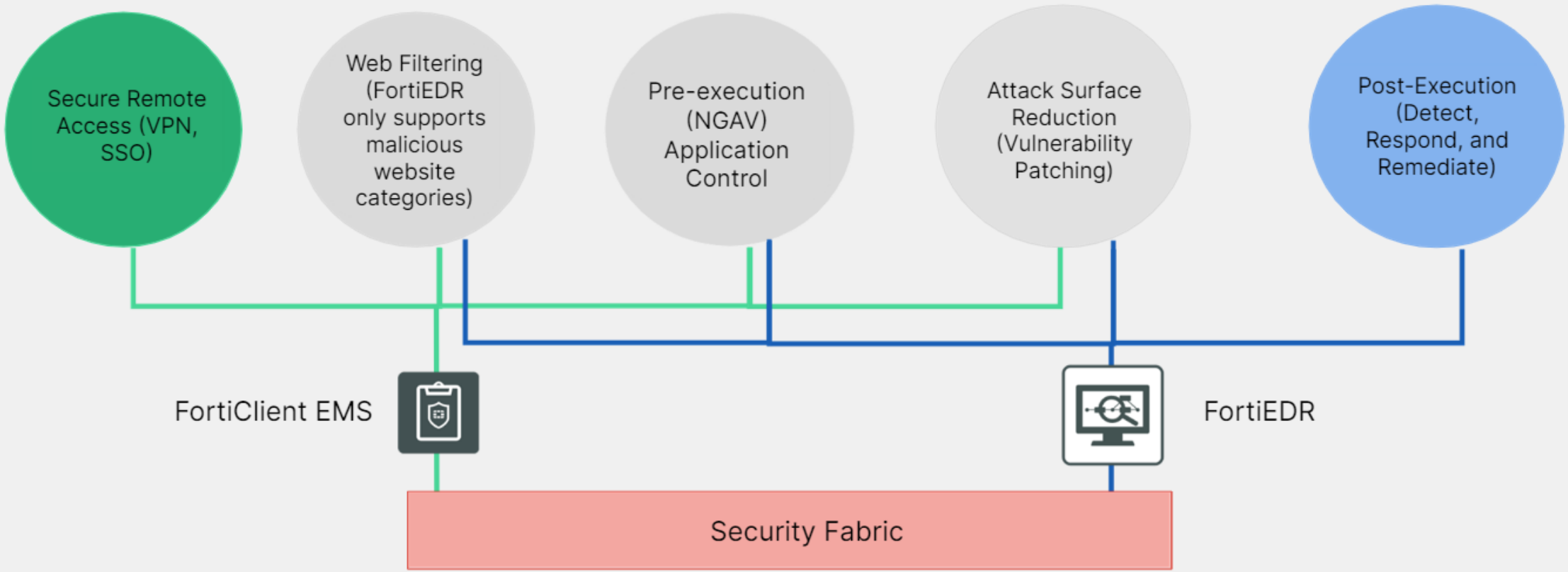
- Єдиний агент для:
  - Доступу (ZTNA, VPN)
  - Захисту ПК (EPP)
  - SASE
  - Digital Experience (DEM)
  - Fabric Support (PAM, NAC, FortiWeb)



© Fortinet Inc. All Rights Reserved.

Набір функцій

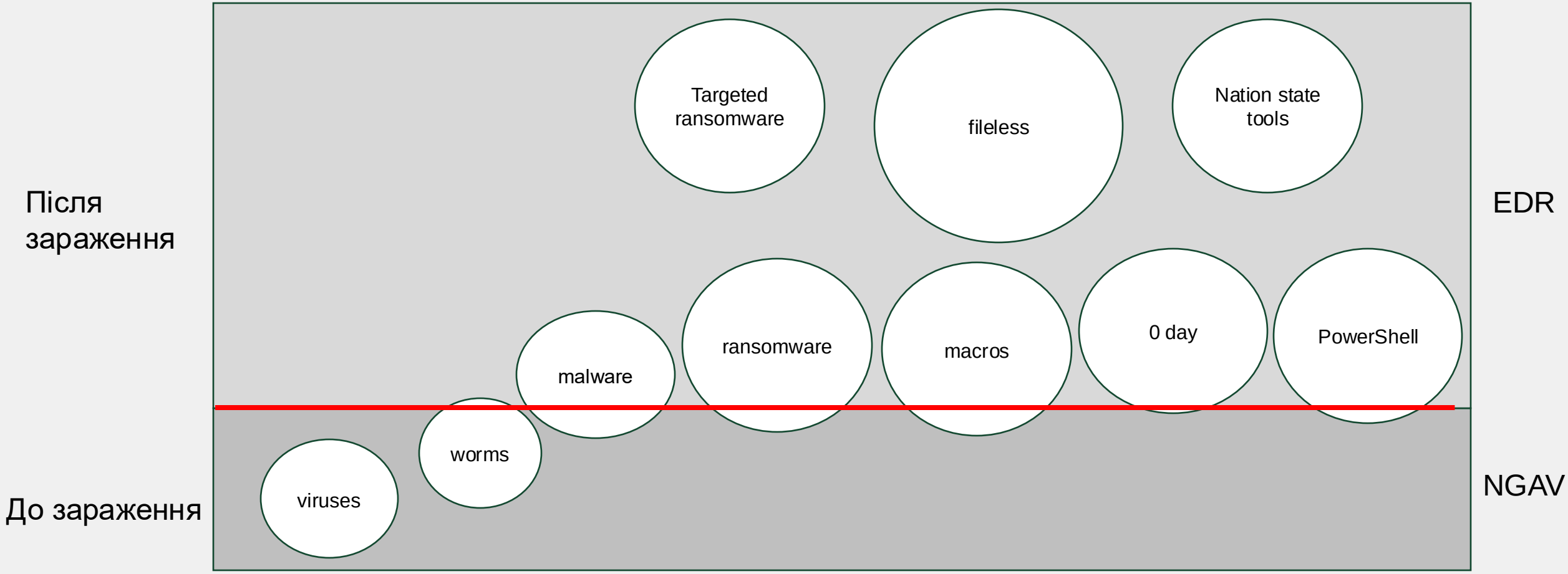
FortiEDR це не тільки ПК співробітників



© Fortinet Inc. All Rights Reserved.

Детальніше щодо захисту

Від чого захищає EDR



© Fortinet Inc. All Rights Reserved.

Операційні системи

FortiEDR це не тільки ПК співробітників

FortiClient

Supported Operating Systems
Microsoft Windows 7 (32-bit and 64-bit)
Microsoft Windows 8, 8.1 (32-bit and 64-bit)
Microsoft Windows 10 (32-bit and 64-bit)
Microsoft Windows 11 (64-bit)
Microsoft Windows Server 2012 or later
macOS 10.14 or later
iOS 9.0 or later
Android 5.0 or later
Linux Ubuntu 16.04 and later, Red Hat 7.4 and later, CentOS 7.4 and later with KDE or GNOME
All Chromebook versions

FortiEDR

Supported Platforms

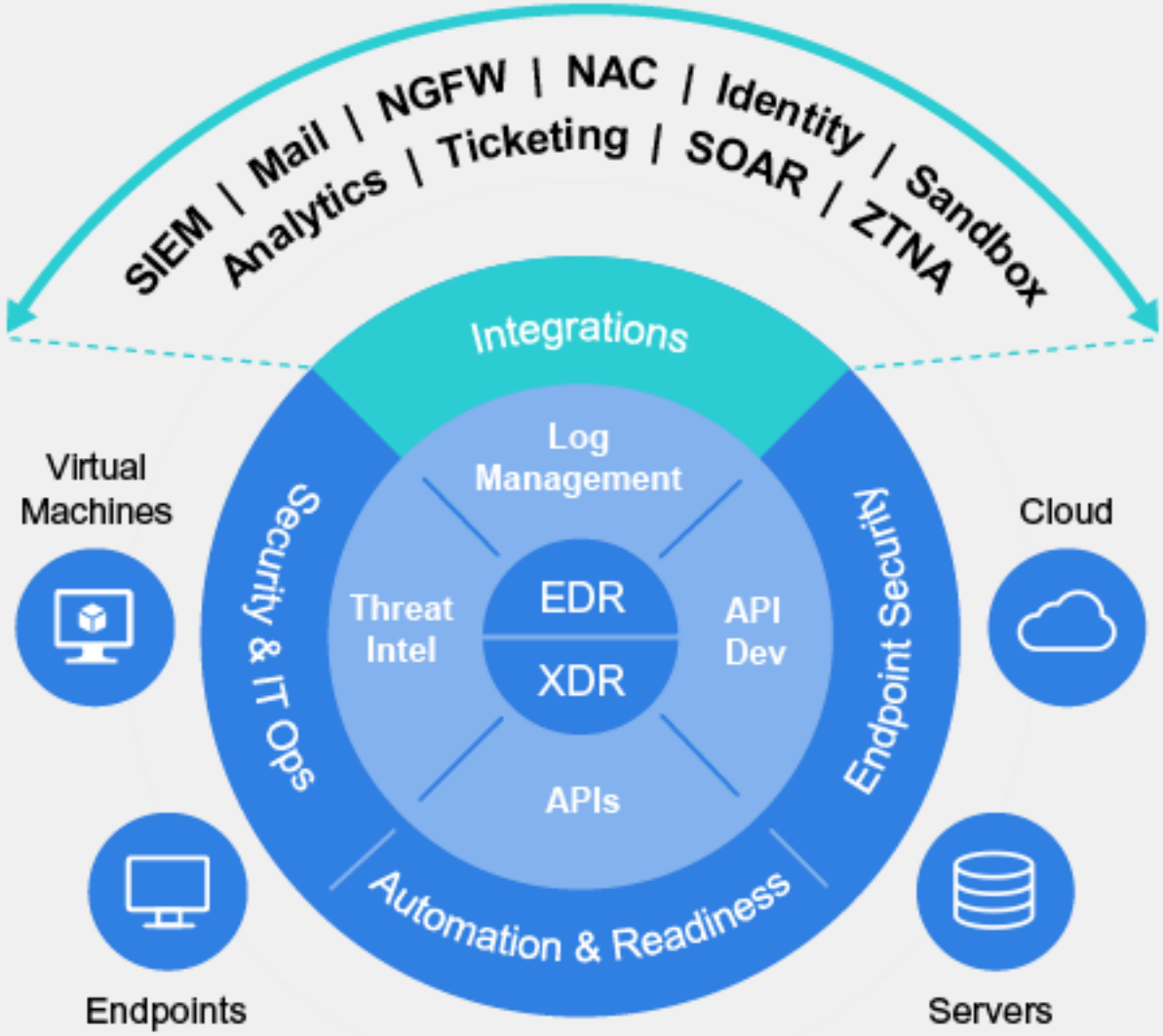
- Windows XP SP2, 7, 8, 8.1, 10, and 11 (32-bit and 64-bit versions)
- Windows Server 2003 SP2, R2 SP2, 2008 SP1, 2008 R2 SP2, 2012, 2012 R2, 2016, 2019, and 2022
- MacOS Versions: El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14), Catalina (10.15), Big Sur (11), Monterey (12), Ventura (13), and Sonoma (14)
- Linux Versions: RedHat Enterprise Linux and CentOS 6.8+, 7.2+, 8+, and 9+
  Ubuntu LTS 16.04.5+, 18.04/ 20.04/and 22.04 server, 64-bit only
  Oracle Linux 6.10, 7.7+, and 8.2+
  Amazon Linux AMI 2 2018
  Open SUSE Leap 15.2
  SUSE Linux Enterprise Server SLES v12 SP5 and v15
  RedHat 9
- VDI Environments: VMware Horizons 6 and 7, and Citrix XenDesktop 7
- Google Cloud Marketplace enablement for all supported OS platforms

© Fortinet Inc. All Rights Reserved.

Основи FortiEDR

Комплексне рішення захисту кінцевих пристроїв

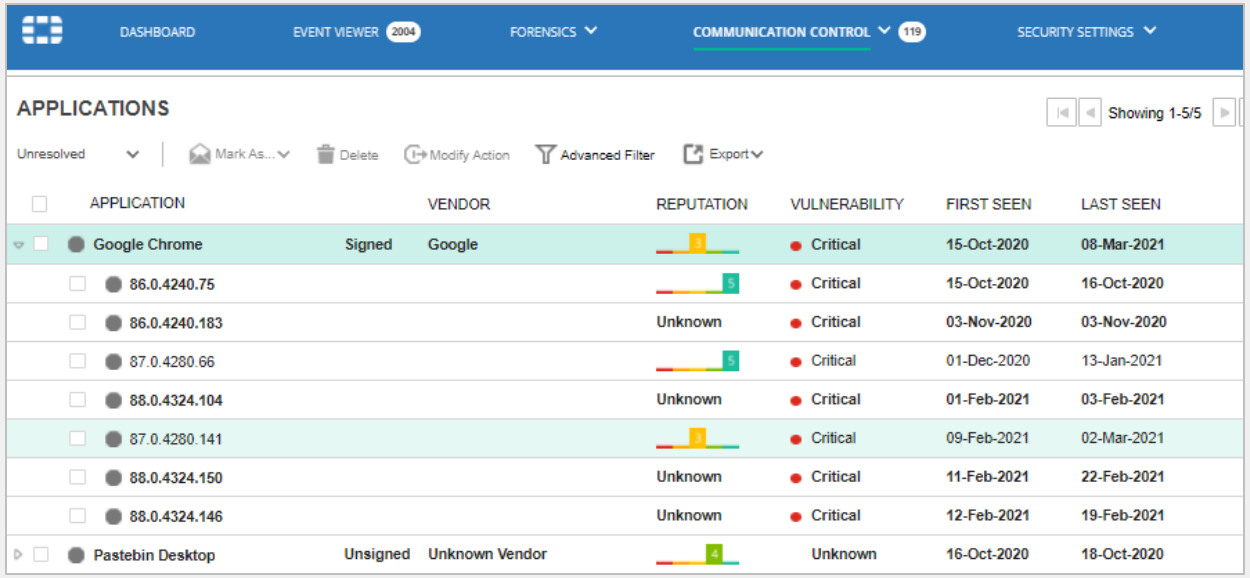
- Єдиний «легкий» агент
- ML та поведінковий аналіз
- Класифікація за допомогою хмарного AI
- Працюємо з застарілими ОС та гібридними середовищами
- Віддалена протидія
- Захищений від втручання
- Інтеграція з іншими вендорами

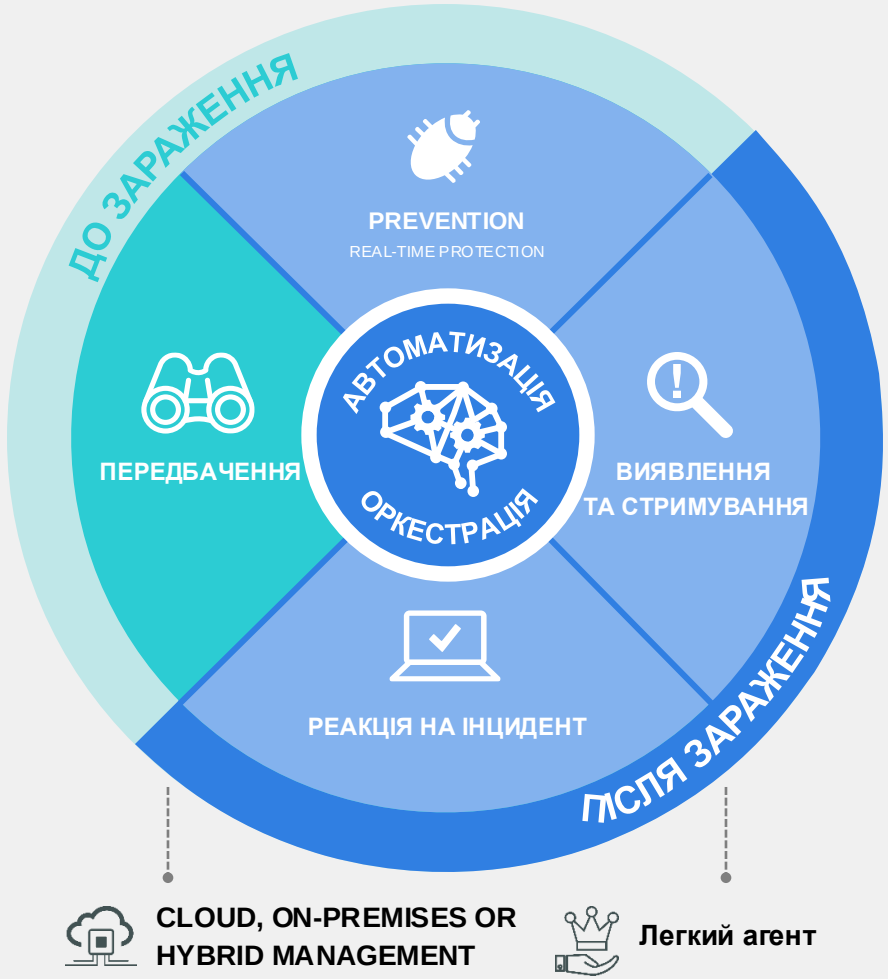


© Fortinet Inc. All Rights Reserved.

Проактивне зменшення площі атаки

- Шкідливі та IoT пристрої
- ПЗ, вразливості, CVE та доповнення рейтингу програм
- Virtual patching
- Політики контролю ПЗ





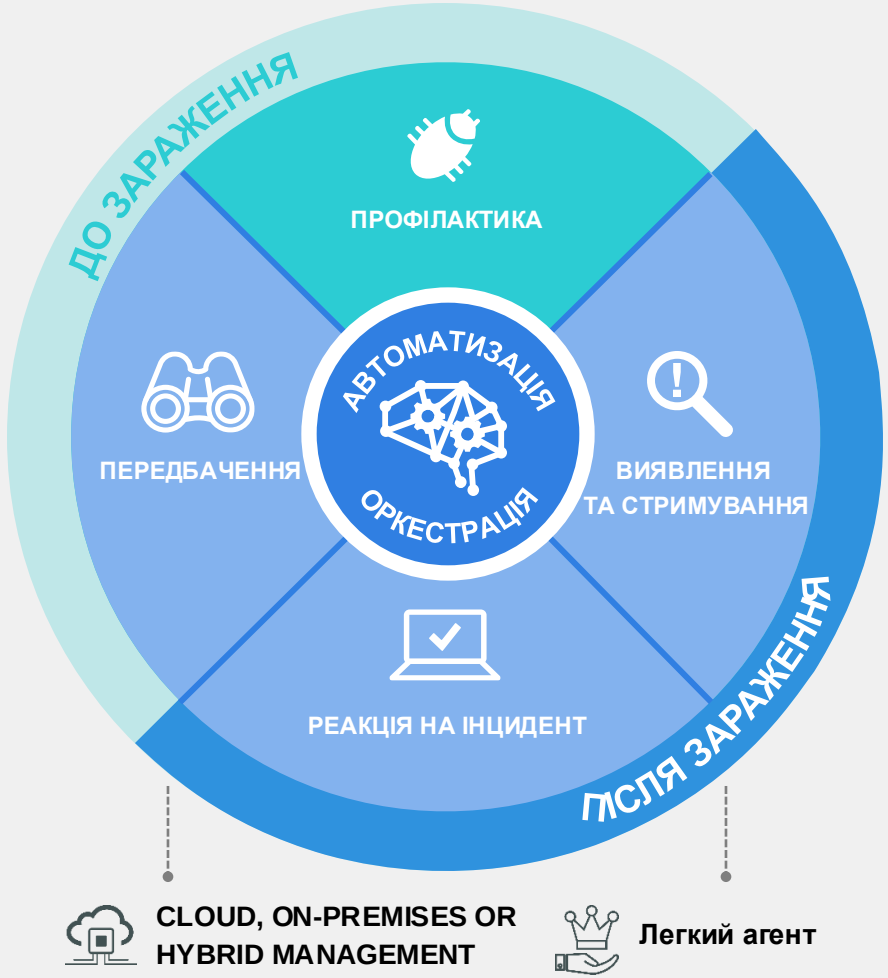
© Fortinet Inc. All Rights Reserved.

Профілактика

Протидія в реальному часі

- Машинне навчання, NGAV на рівні ядра
- Постійні оновлення від FortiGuard
- Захист в реальному часі та «відкат» зашифрованих файлів
- Інтеграція з пісочничею

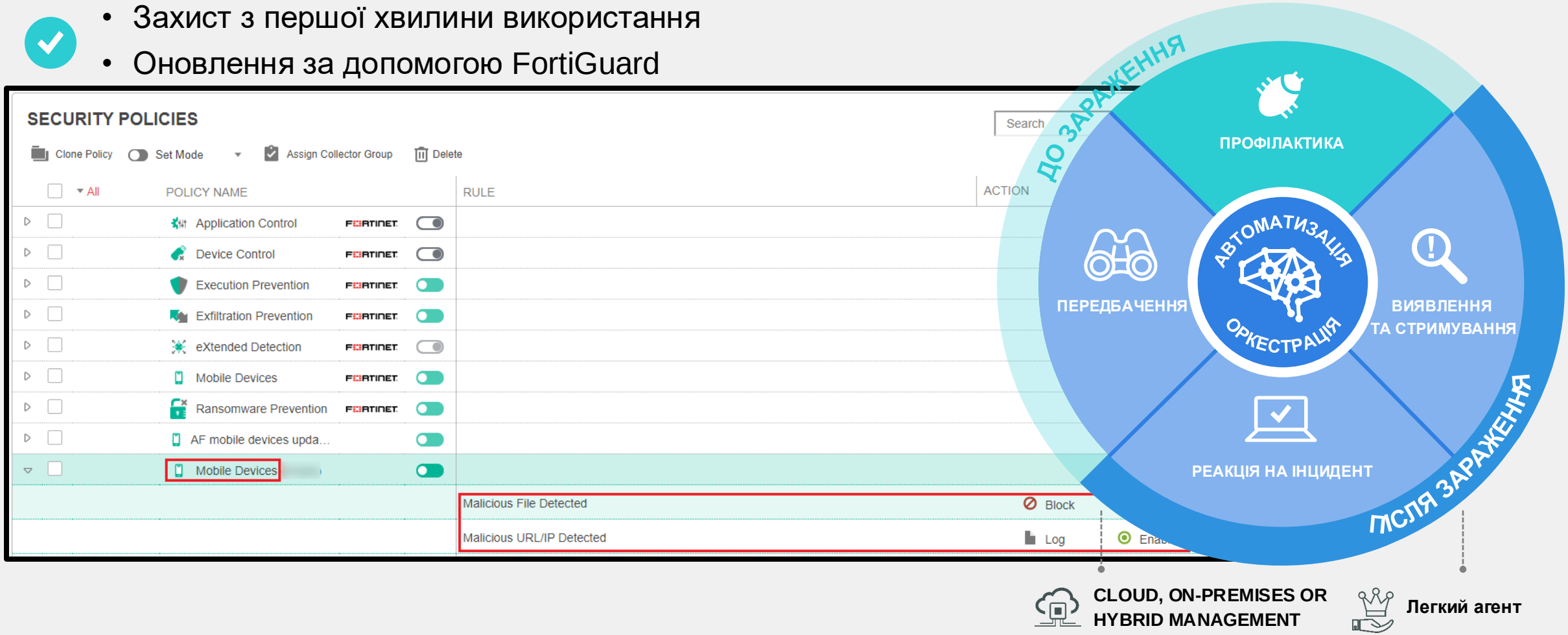
https://www.fortinet.com/blog/threat-research/guard-your-drive-from-driveguard



© Fortinet Inc. All Rights Reserved.

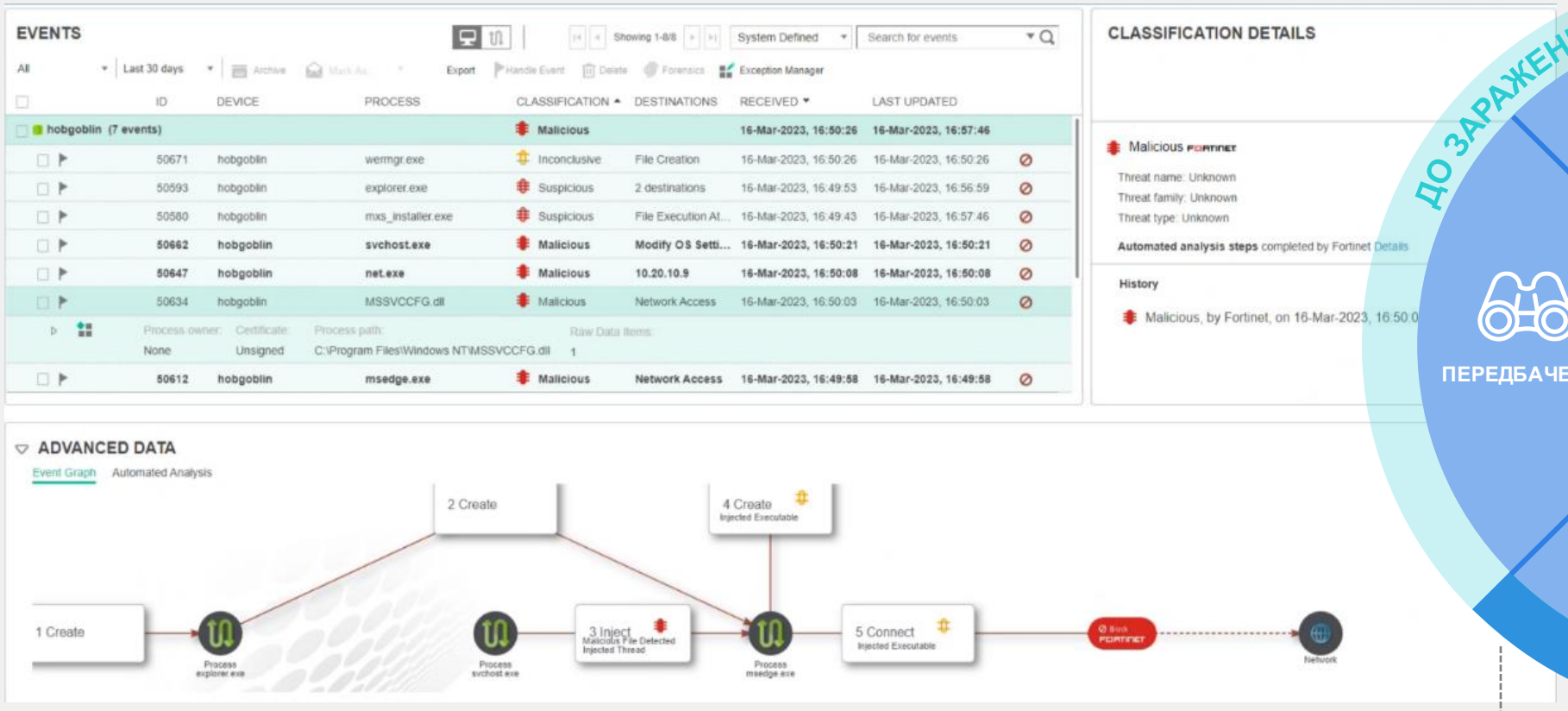
Вбудовані політики безпеки

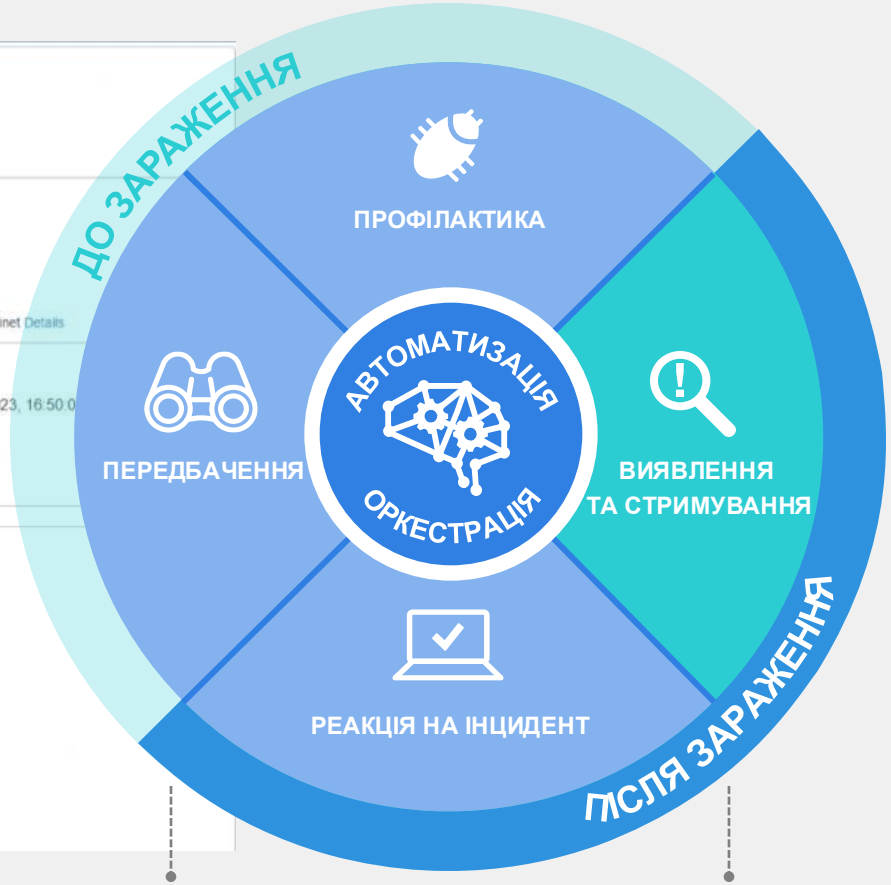
- Захист з першої хвилини використання
- Оновлення за допомогою FortiGuard



© Fortinet Inc. All Rights Reserved.

Виявлення та блокування





CLOUD, ON-PREMISES OR HYBRID MANAGEMENT

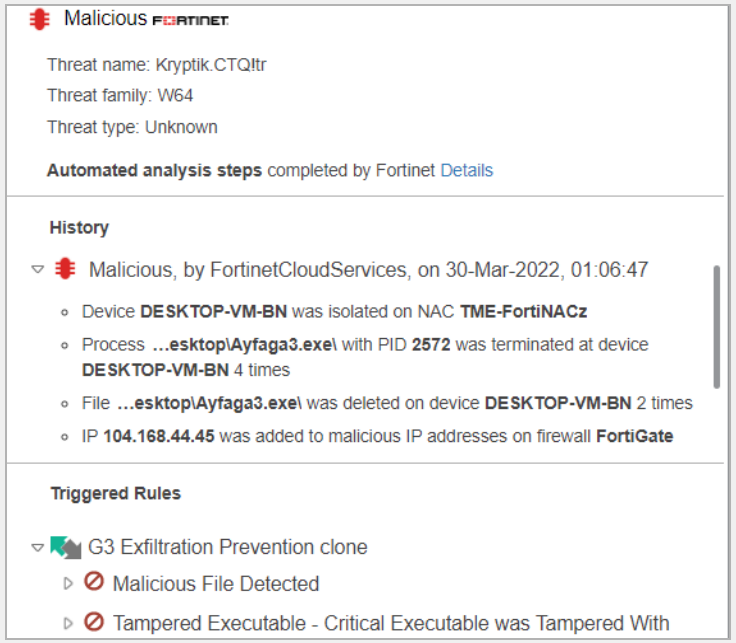
Легкий агент

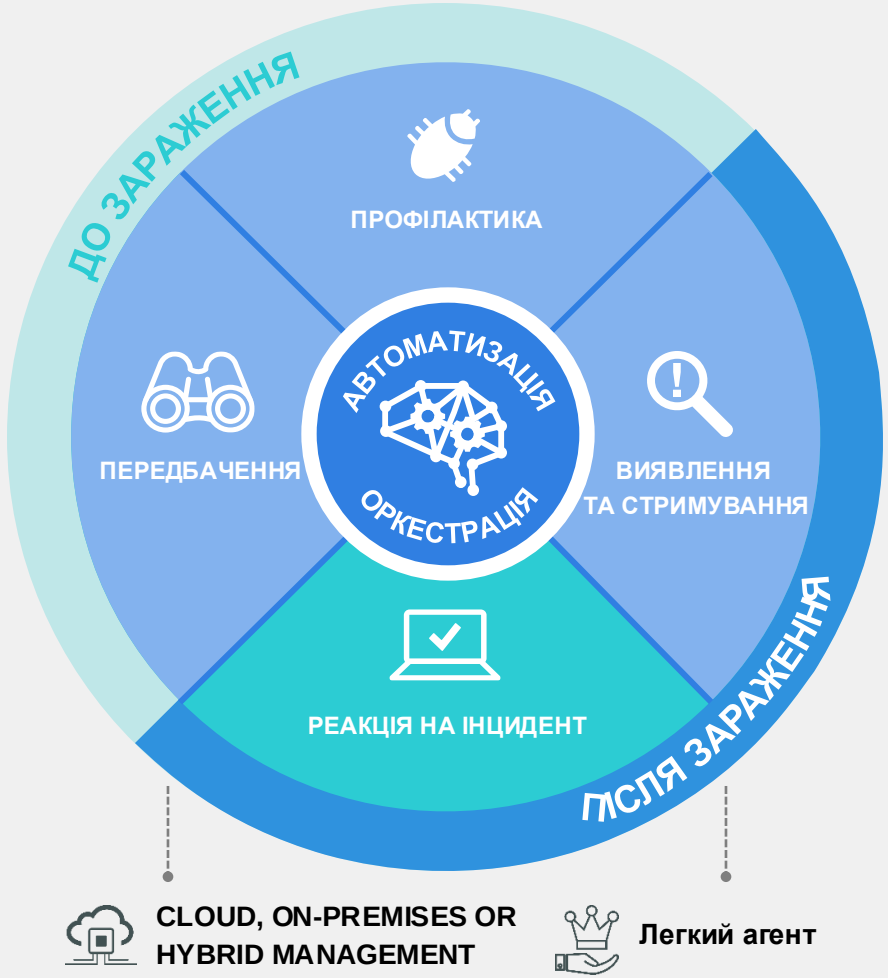
© Fortinet Inc. All Rights Reserved.

Автоматизовані реакції

Реагування на інциденти
Fortinet Ref.: 19154; FORT-035200

- Кастомізовані сценарії (playbooks) на основі груп пристроїв та класу загрози
- Розширена (eXtended) автоматизація реакції
- Інтеграція з іншими виробниками

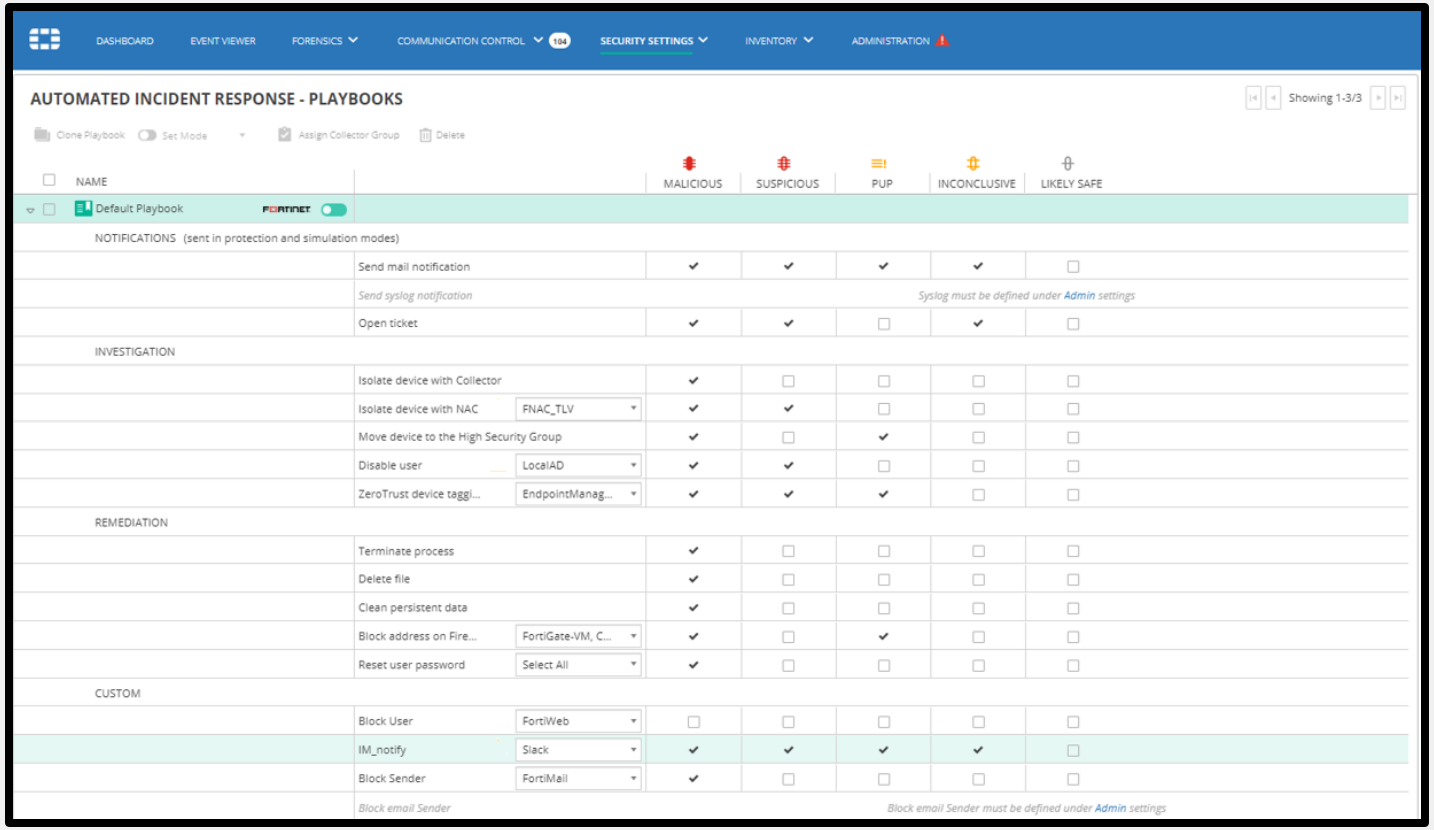


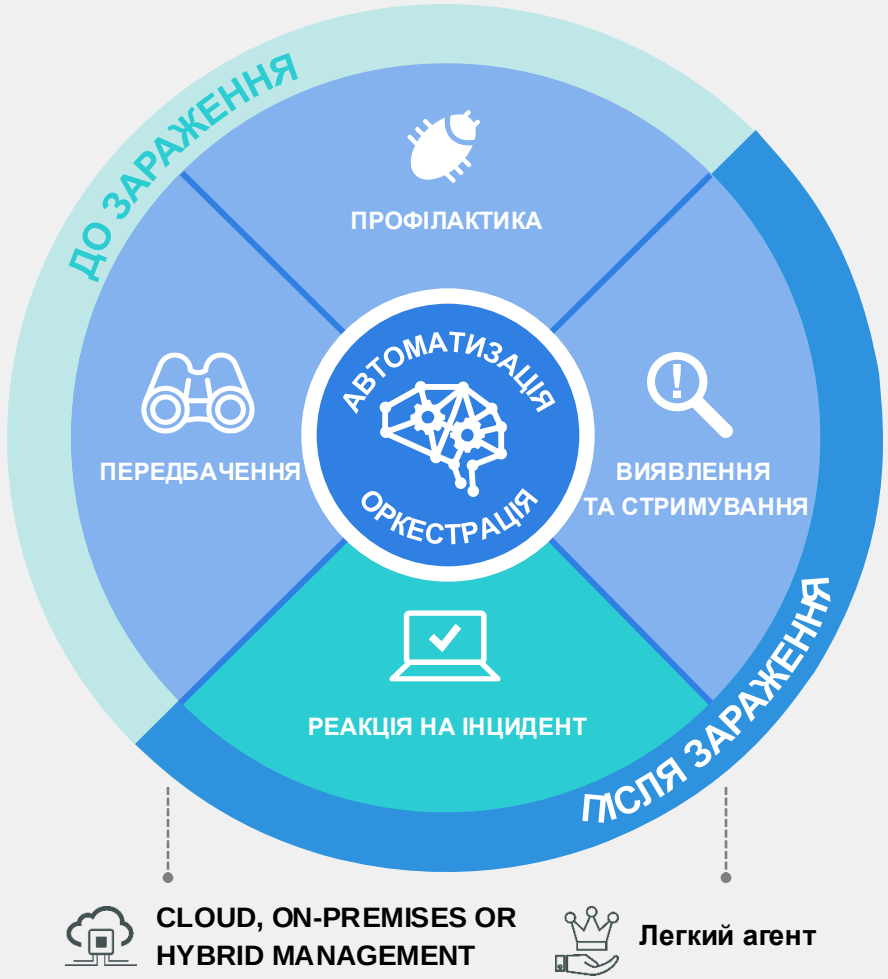


© Fortinet Inc. All Rights Reserved.

Різні реакції на різні рівні критичності

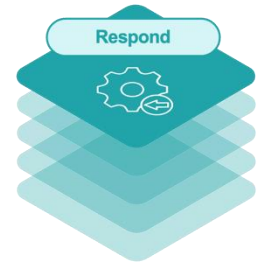
- Різні playbook для різного рівня загроз
- Налаштування сповіщень та протидії
- Протидія за допомогою як інструментів Fortinet так і сторонніх

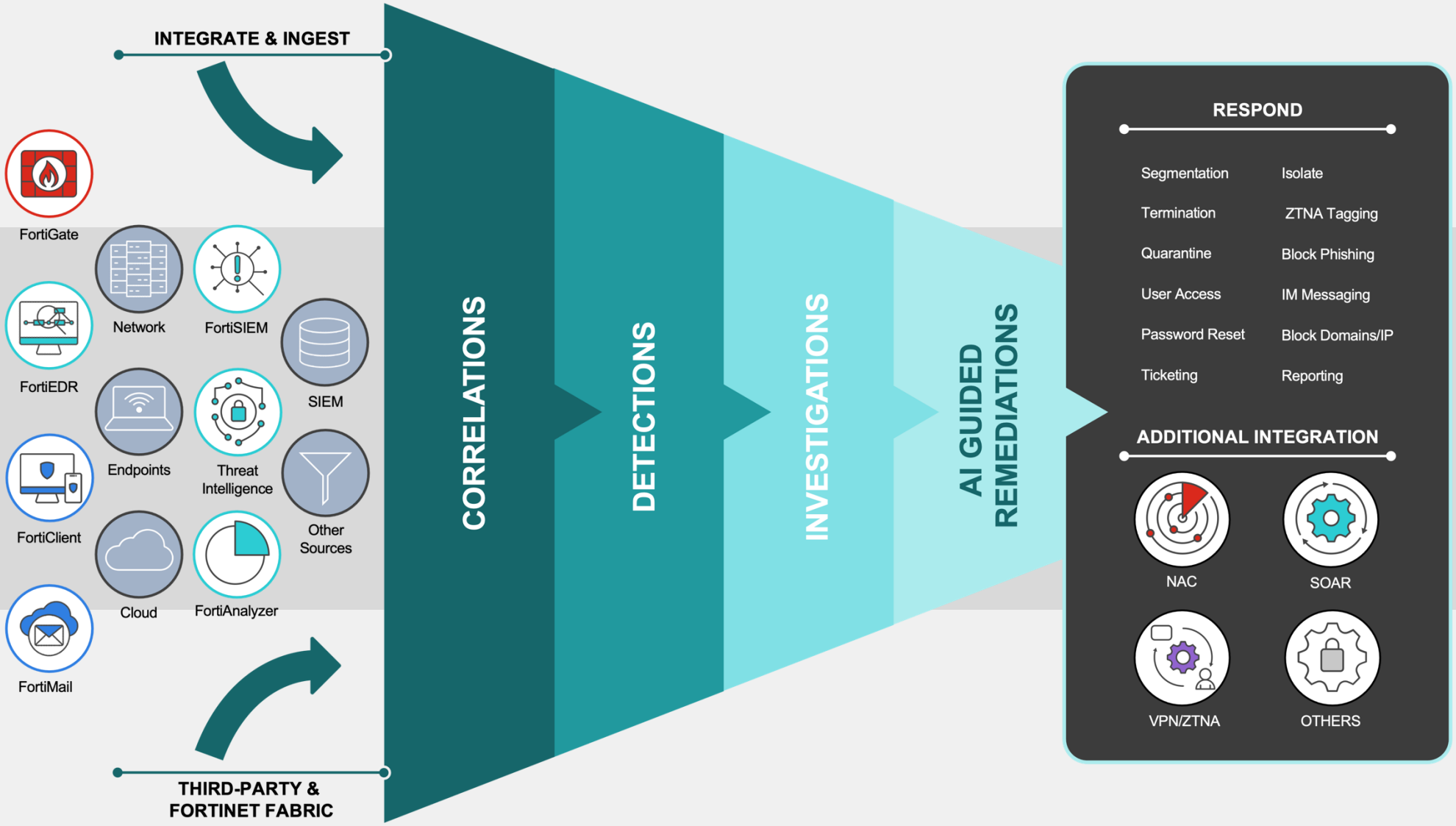




© Fortinet Inc. All Rights Reserved.

В чому відмінність EDR від XDR





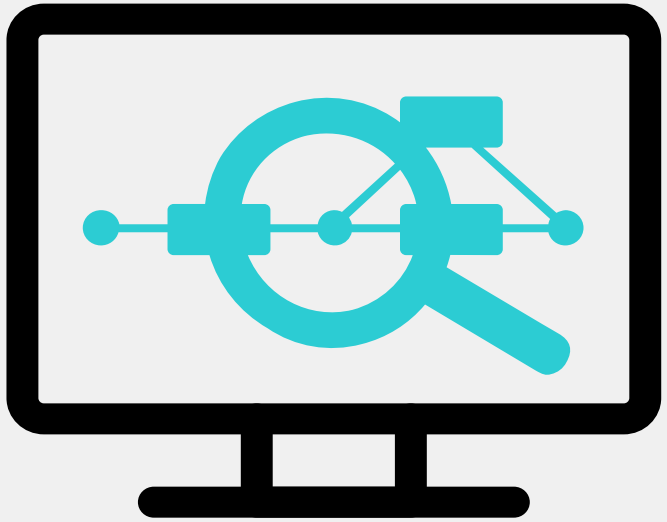
© Fortinet Inc. All Rights Reserved.

Ліцензування FortiEndpoint

FortiEndpoint

FortiClient

+



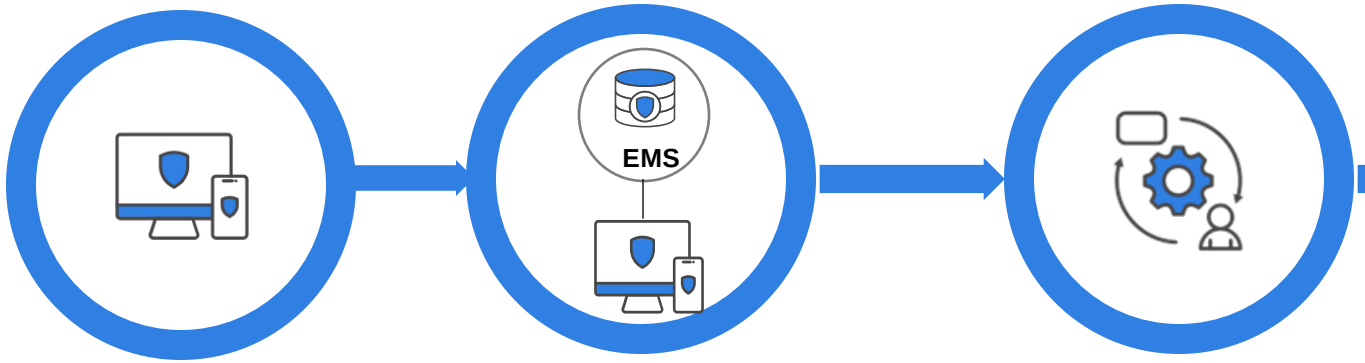
FortiXDR

© Fortinet Inc. All Rights Reserved.

Уніфікований агент

Постійні інновації і 20M інстальованих агентів

Безпечний доступ



FortiClient VPN

- Традиційний VPN
- Free FortiClient

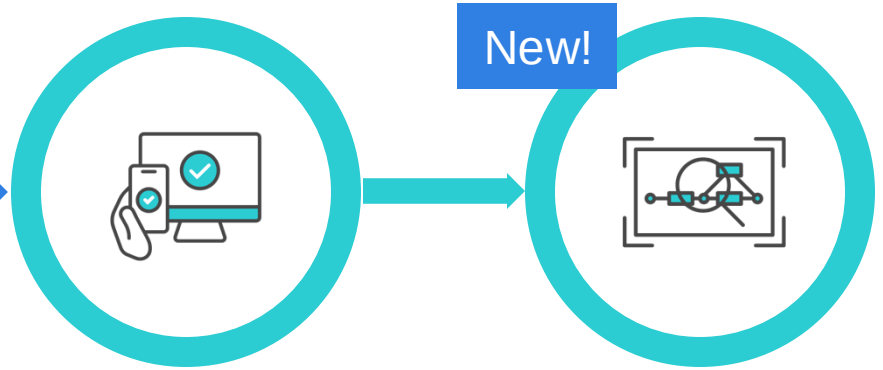
Видимість ПК (SaaS / On-prem)

- Централізоване керування
- Видимість та телеметрія

Універсальний ZTNA

- Постійна перевірка
- Контроль вразливостей
- Контроль інтернету

Інтегрована безпека



Endpoint Protection (EPP)

- Антивірус з AI
- Application firewall
- Захист від шифрувальщиків

Endpoint Detection and Response (EDR)

- Поведінковий захист
- Розширення автоматизація
- Полювання на загрози

© Fortinet Inc. All Rights Reserved.

Формфактори FortiEndpoint

Апаратні рішення

- Perpetual

Віртуальні машини

- Perpetual
- Subscription

Public Clouds

- BYOL
  - Perpetual
  - Subscription
- PAYG

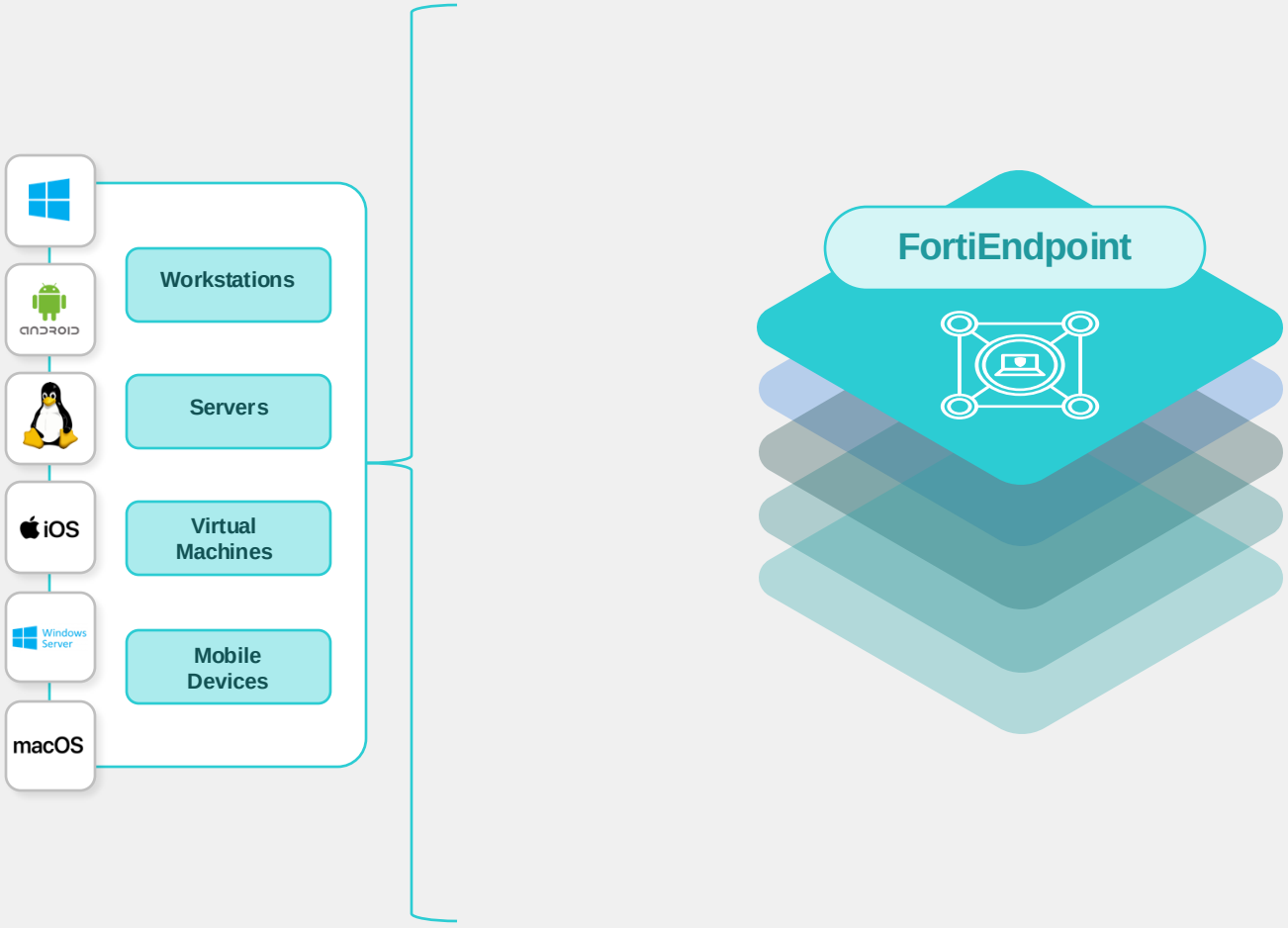
SaaS

- Subscription

© Fortinet Inc. All Rights Reserved.

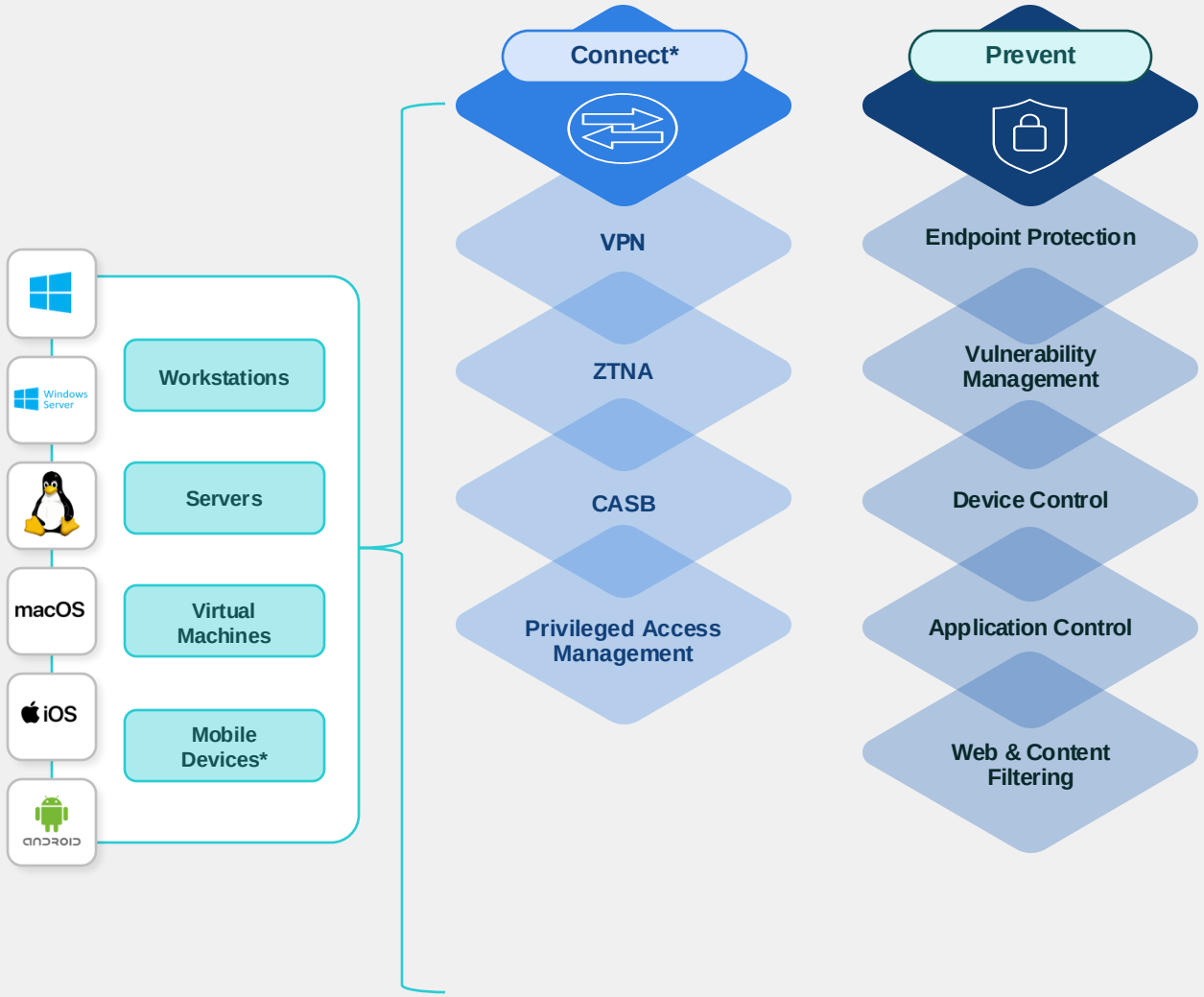
FortiEndpoint – уніфікований агент

Безпека ПК та сервісів



© Fortinet Inc. All Rights Reserved.

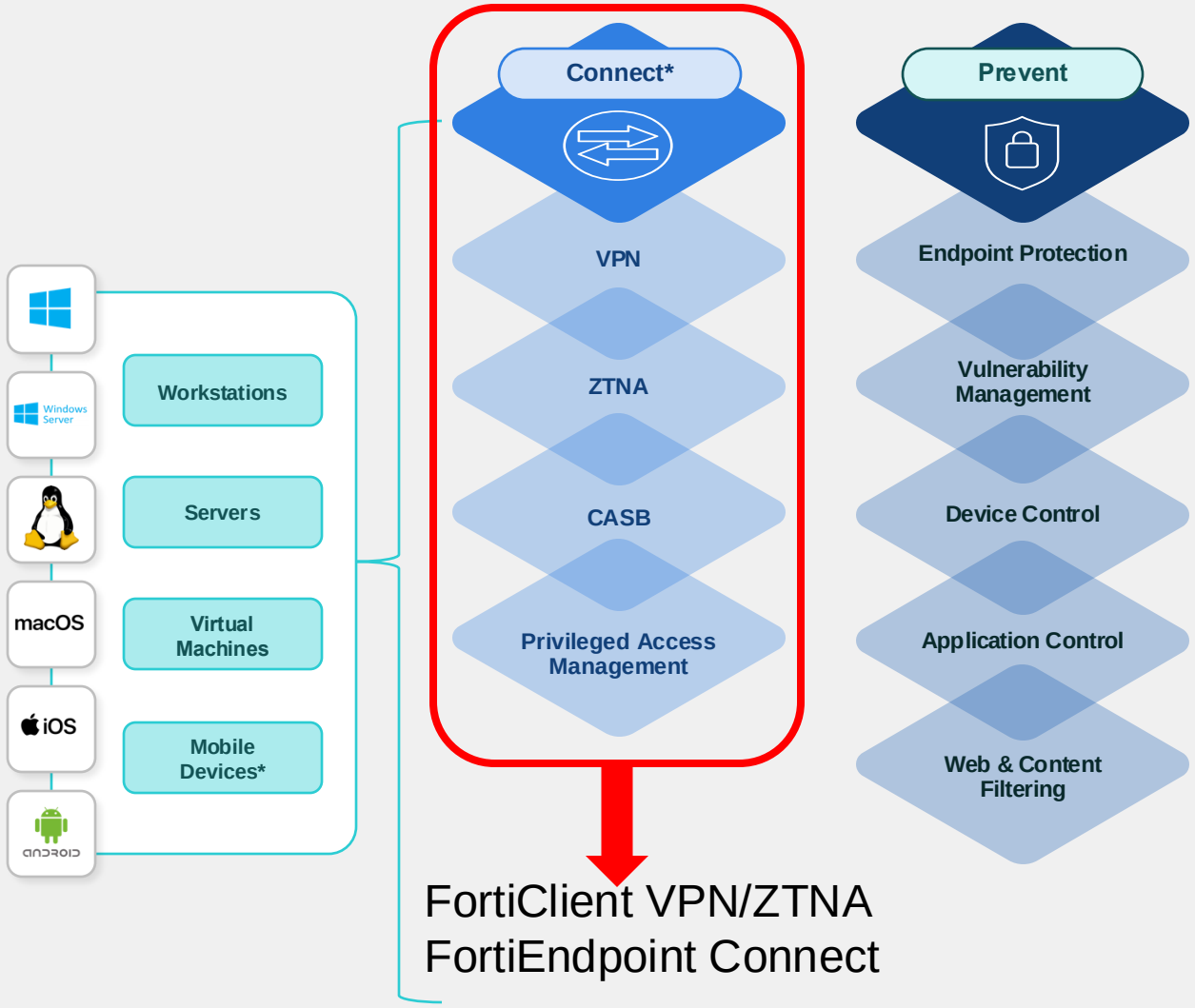
FortiEndpoint – уніфікований агент



* Mobile devices not supported on EDR/XDR bundles

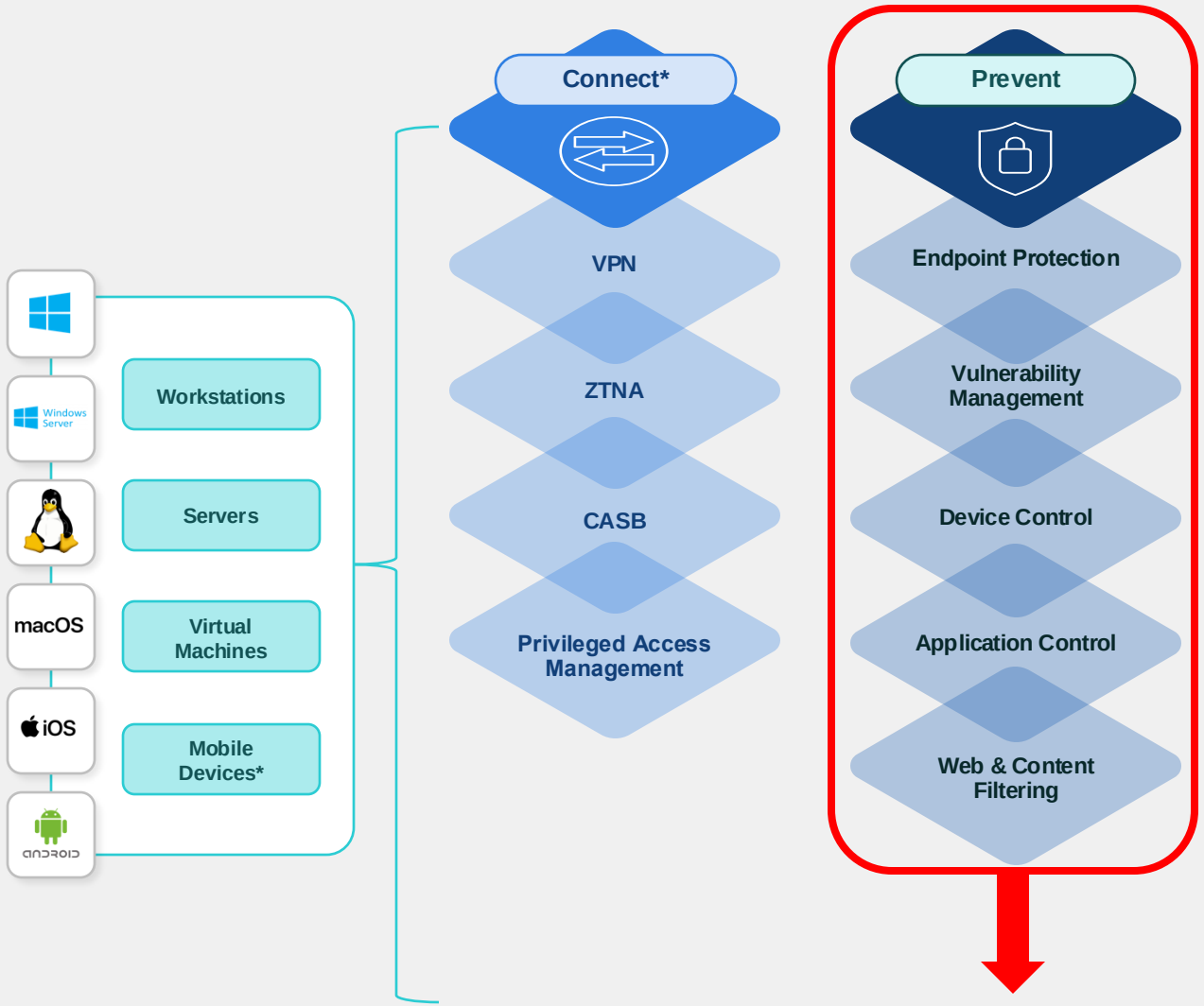
© Fortinet Inc. All Rights Reserved.

The Unified Agent: FortiClient Components of FortiEndpoint



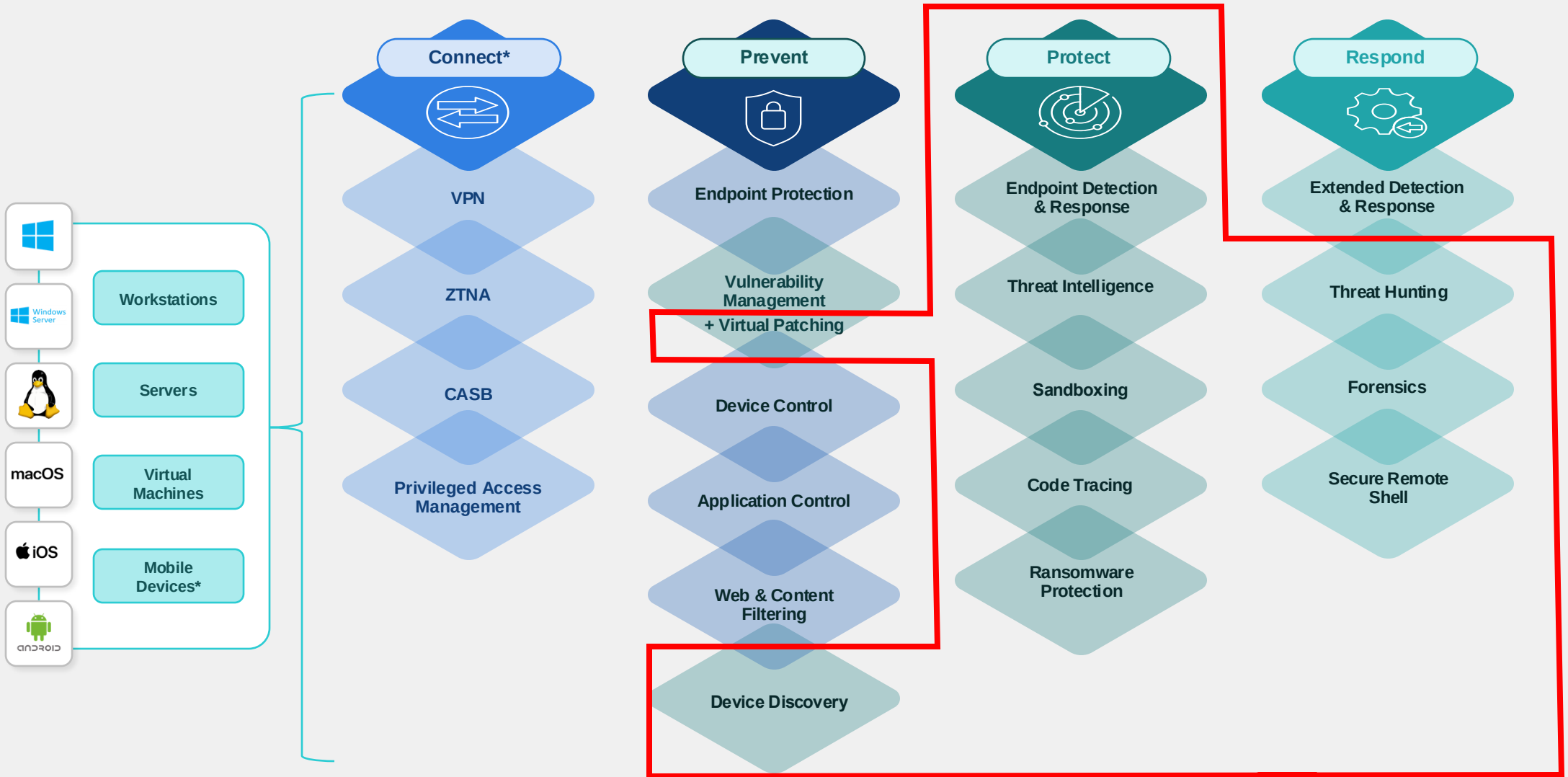
© Fortinet Inc. All Rights Reserved.

The Unified Agent: FortiClient Components of FortiEndpoint



© Fortinet Inc. All Rights Reserved.

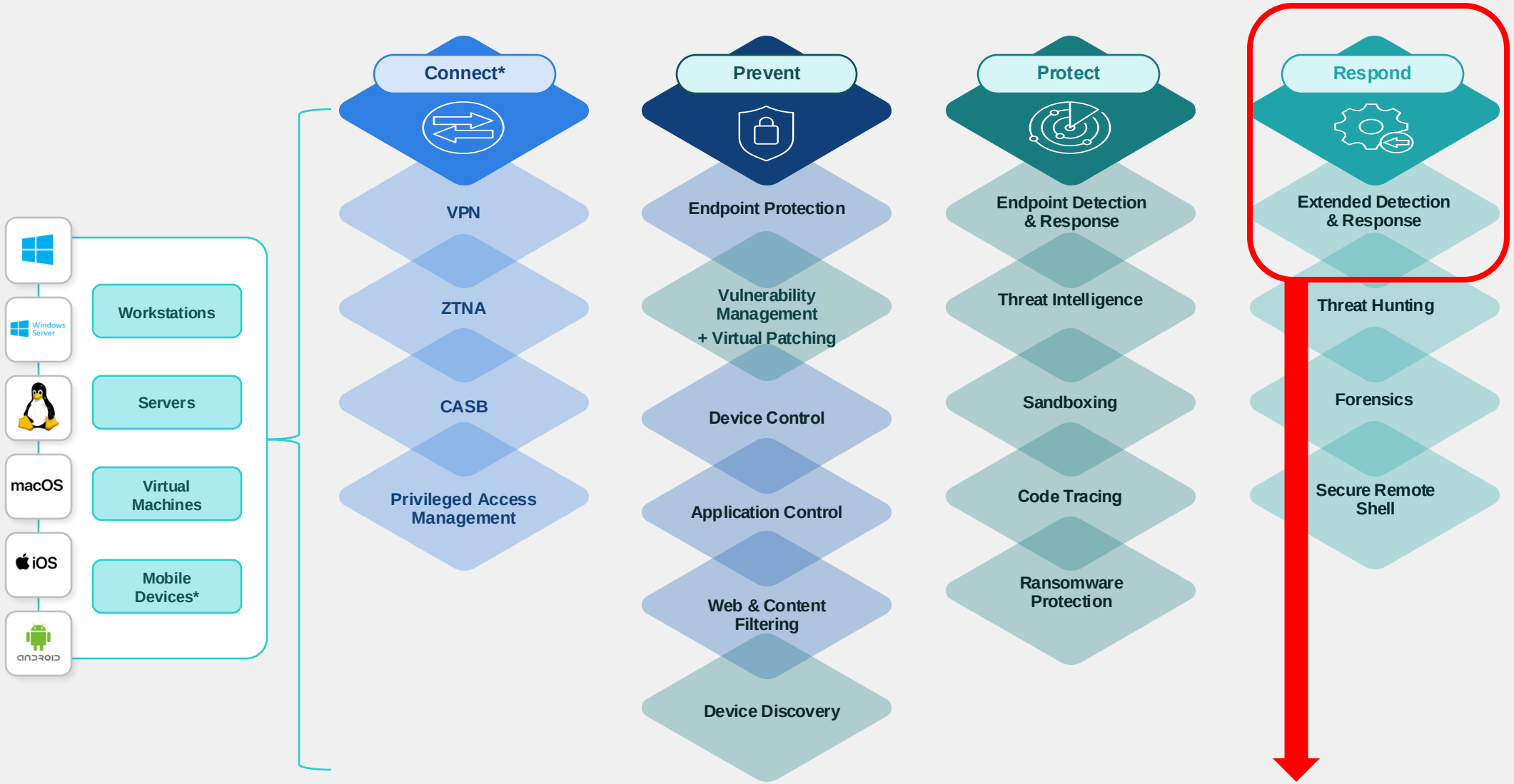
FortiEDR Finds Unmanaged IT and IoT Devices



FortiEDR Discover, Protect, and Respond
FortiEndpoint EDR Essentials

© Fortinet Inc. All Rights Reserved.

FortiEDR Finds Unmanaged IT and IoT Devices



FortiEDR Discover, Protect, & Respond and XDR
FortiEndpoint XDR

© Fortinet Inc. All Rights Reserved.

Order guide

	PREVENT	EDR ESSENTIALS	XDR
Features			
Zero Trust Connectivity			
ZTNA Agent	✓	✓	✓
VPN	✓	✓	✓
Vulnerability Scan and Remediation	✓	✓	✓
FortiGuard Web and Video Filtering	✓	✓	✓
API-based and Inline CASB (Saas)	✓	✓	✓
Endpoint Protection Platform (EPP)			
EPP	✓	✓	✓
Sandbox	✓	✓	✓
Extended Detection & Response (EDR/XDR)			
Discover		✓	✓
Protect		✓	✓
Respond		✓	✓
XDR			✓
Security Operations Center (SOC)			
Forensics		included with managed service	
SOCaaS			
Deployment			
Managed	✓	✓	✓
Central Logging and Reporting			
FortiAnalyzer Cloud (SaaS)*	✓	✓	✓
Additional Services			
Best Practice Service (BPS) Consultation**	Account add-on	Account add-on	Account add-on

* FortiAnalyzer Cloud does not support EDR logs.
** BPS is mandatory for all solutions that include EDR.

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortiendpoint.pdf

© Fortinet Inc. All Rights Reserved.

Order guide

The following summarizes offerings for managed packages. All managed packages include Forensics and SOCaaS.

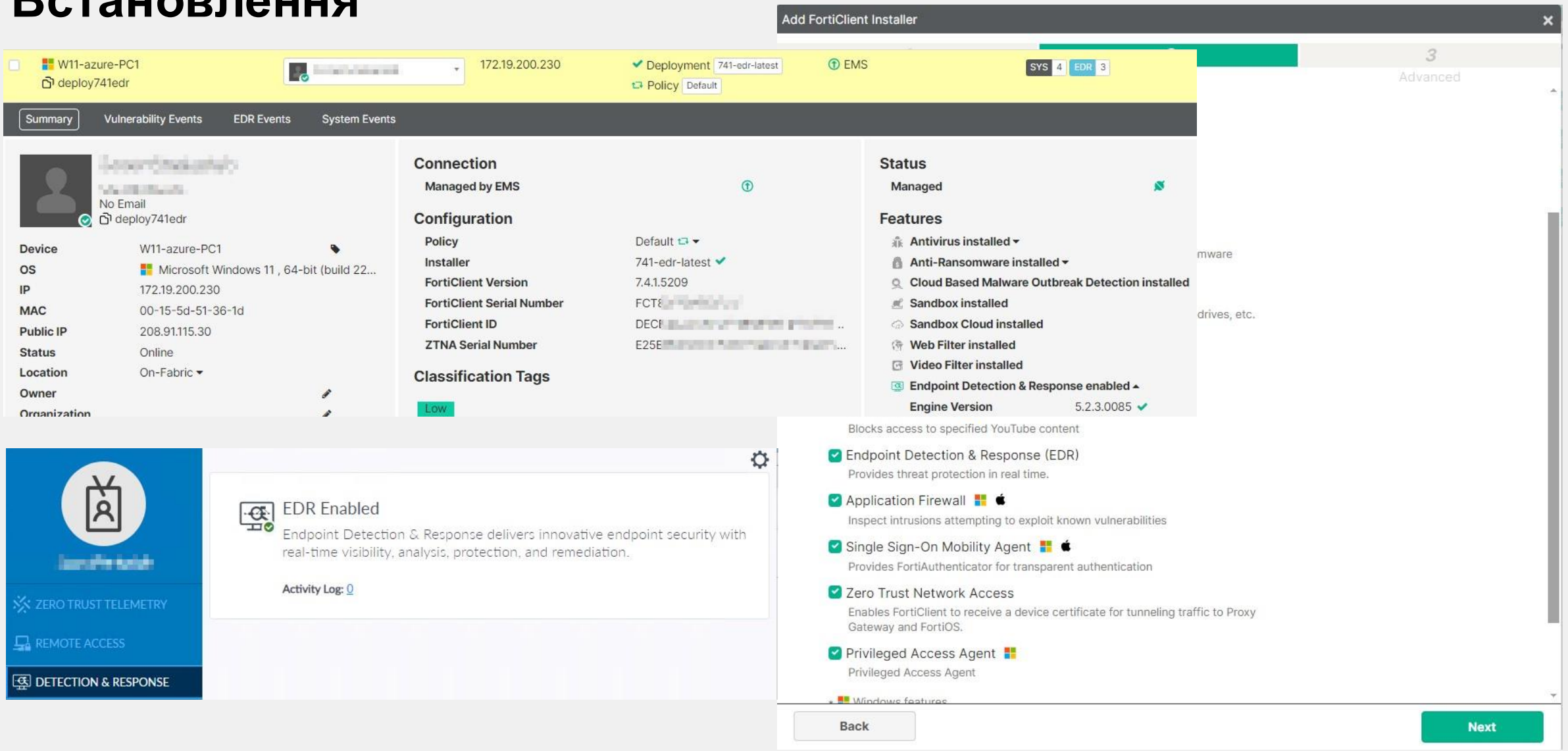
	PREVENT	EDR ESSENTIALS	XDR
Features			
Zero Trust Connectivity			
ZTNA Agent	✓	✓	✓
VPN	✓	✓	✓
Vulnerability Scan and Remediation	✓	✓	✓
FortiGuard Web and Video Filtering	✓	✓	✓
API-based and Inline CASB (Saas)	✓	✓	✓
Endpoint Protection Platform (EPP)			
EPP	✓	✓	✓
Sandbox	✓	✓	✓
Extended Detection & Response (EDR/XDR)			
Discover		✓	✓
Protect		✓	✓
Respond		✓	✓
XDR			✓
Security Operations Center (SOC)			
Forensics		included with managed service	
SOCaaS			
Deployment			
Managed	✓	✓	✓
Central Logging and Reporting			
FortiAnalyzer Cloud (SaaS)*	✓	✓	✓
Additional Services			
Best Practice Service (BPS) Consultation**	Account add-on	Account add-on	Account add-on

* FortiAnalyzer Cloud does not support EDR logs.
** BPS is mandatory for all solutions that include EDR.

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortiendpoint.pdf

© Fortinet Inc. All Rights Reserved.

Встановлення



https://docs.fortinet.com/document/fortiendpoint/latest/administration-guide/189694/creating-a-fortiendpoint-installer

© Fortinet Inc. All Rights Reserved.

Як можна ознайомитись?

- пілот
- демо

Євгеній Таран, Systems Engineer
ytaran@fortinet.com