



FortiEndpoint. Уніфікований захист ПК співробітників

Євгеній Таран, Systems Engineer
ytaran@fortinet.com



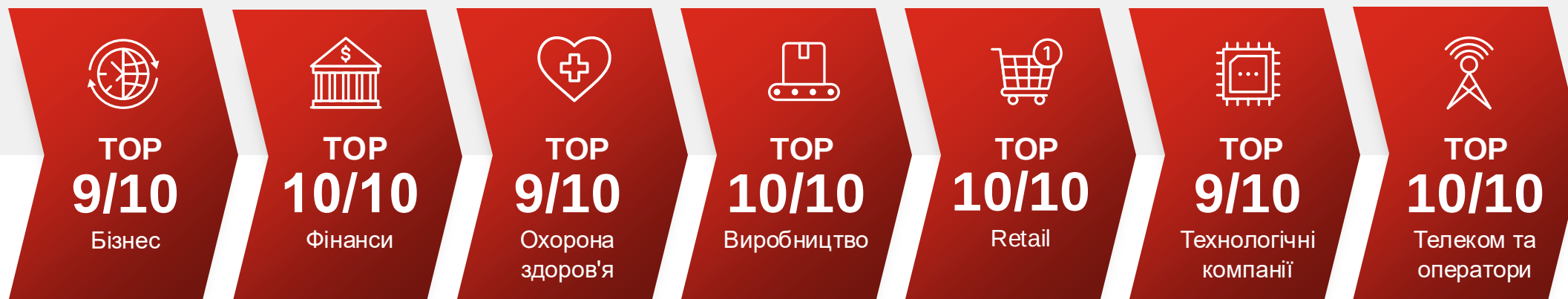
Вступ





Перша довірена компанія кібербезпеки з США

Fortinet зайняв 7 місце серед компаній яким довіряє Forbes

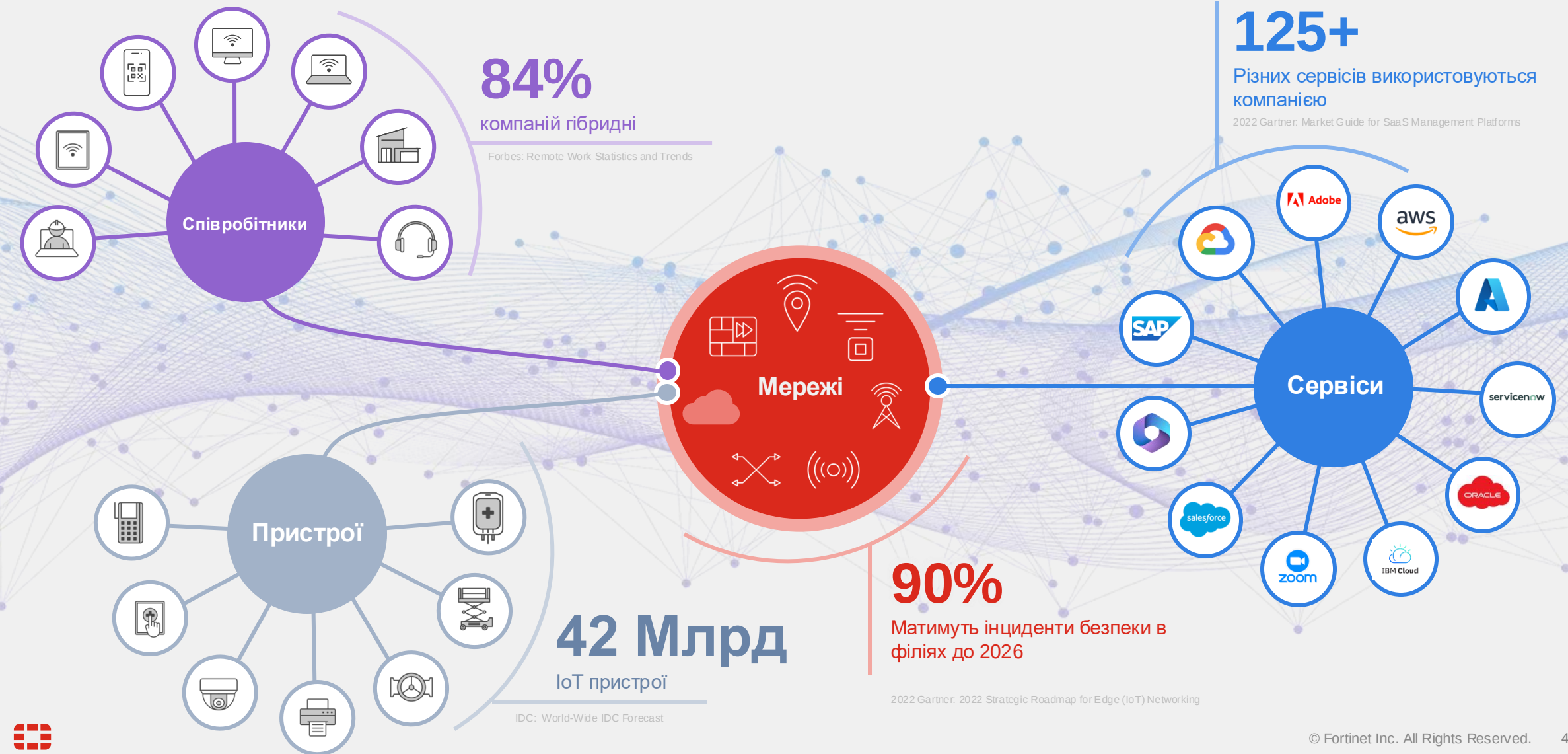


Fortinet захищає **більше 805,000** компаній світу

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



Децентралізація та нульова довіра





Платформа кібербезпеки від Fortinet



Secure Networking

- FortiGate**
NGFW with ASIC acceleration and industry leading Convergence
- FortiSwitch**
Protected Ethernet connectivity via Secure Networking convergence with FortiGate
- FortiAP**
Protected Wi-Fi connectivity via Secure Networking convergence with FortiGate
- FortiManager**
Centralized management of your Fortinet security infrastructure
- FortiNAC**
Visibility, access control and automated responses for all networked devices
- FortiExtender**
Extend scalable and resilient LTE and LAN connectivity
- FortiGate Cloud**
SaaS platform offering zero-touch deployment, network management and security analytics
- FortiEdge Cloud**
Cloud management for standalone LAN, WLAN and 5G gateway equipment
- FortiAIops**
AI based insights for rapid analysis and remediation of network issues
- FortiFone**
Robust IP phones and softclient to stay connected from anywhere
- FortiVoice**
Unified communications with secure voice, chat, conferencing, and fax
- FortiCamera**
Physical security with intelligent motion detection in any light condition
- FortiRecorder**
Secure NVR with smart AI analysis and centralized visibility
- FortiConverter**
Secure and automated firewall migration from a broad spectrum of vendors
- FGaaS**
Hardware as a service for FortiGate



Resources

- Product Matrix**
Specifications for top selling models
- Fortinet Brochure**
Highlighting our broad, integrated, and automated solutions, quarterly
- Free Training**
Fortinet is committed to training over 1 million people by 2025
- Free Assessment**
Perform an assessment in your network to validate your existing controls
- FortiOS**
The Heart of the Fortinet Security Fabric
- 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
- FortiClient EPP Agent**
Endpoint Protection Agent with AV, URL and Sand-box
- FortiSASE**
Cloud-delivered Security Services Edge
- FortiProxy**
Enforce internet compliance and granular application control
- FortiMonitor**
SaaS based DEM platform, performance monitoring
- FortiCASB**
Prevent misconfigurations of SaaS apps and meet compliance
- FortiEndpoint**
XDR, ZTNA and EPP as unified agent

CLOUD

- FortiGate VM**
NGFW w/ SOC acceleration and industry-leading secure SD-WAN
- FortiGate CNF**
Hosted cloud-native firewall for simplified cloud network security
- FortiWeb**
Prevent web application attacks against critical web assets
- FortiADC**
Application-aware intelligence for distribution of application traffic
- FortiGSLB**
Ensure business continuity during unexpected network downtime
- FortiDDoS**
Machine-learning quickly inspects traffic at layers 3, 4, and 7
- FortiFlex**
Flexible daily usage-based consumption licensing for a broad catalog of solution
- FortiPoints**
Simplified, flexible licensing for annual contracts, renewals, upgrades, and co-terms



AI-Powered FortiGuard Security

- WF** Web Filtering
- IPS** IPS
- AV** AV
- SBX** Sandbox
- IL MPS** IL MPS
- APP CTRL** Application Control
- ATTK SFFC** Attack Surface
- DLP** DLP
- OT** OT Security Services
- IoC** IoC
- IL CASB** IL CASB



Security Operations

- FortiAnalyzer**
Security Fabric log management, monitoring and response
- FortiMail**
AI-powered, protection against email-borne threats
- FortiSIEM**
Enterprise-wide monitoring, threat detection, and response
- FortiSandbox**
AI-powered real-time protection against unknown and 0-day threats
- FortiEDR/XDR**
Automated endpoint protection and correlated incident response
- FortiToken**
Cloud/HW/Mobile MFA provide passwordless adaptive authentication
- FortiSOAR**
Automated security operations, investigation, and response
- FortiAuthenticator**
Centralized identity and access management solution
- FortiNDR**
AI-driven analysis to detect and respond to threats
- FortiGuard MDR Service**
Managed threat detection, investigation, and response
- SOaaS**
Continuous security monitoring, incident triage, and escalation
- FortiRecon**
Proactive digital risk protection service and external/internal threat monitoring
- IR Services**
Rapid detection, containment, and recovery of cyberattacks
- FortiPAM**
Privileged identity and access management, and session monitoring
- FortiDeceptor**
Active deception platform for early in-network attack detection and response
- FortiTester**
Network performance testing and breach attack simulation (BAS)
- FortiTrust Identity**
Identity and Access Management as a Service (IDaaS)
- FortiDevSec**
Orchestrated and automated continuous application security testing
- FortiGuest**
Access management solution for temporary access to guests and visitors
- FortiDAST**
Automated black-box dynamic application security testing
- FortiCNAPP**
Secure code to cloud with a single, data-driven platform
- FortiScanner Cloud**
Cyber Asset Attack Surface Management Service
- FortiNextDLP**
Endpoint DLP and Insider Risk management
- 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



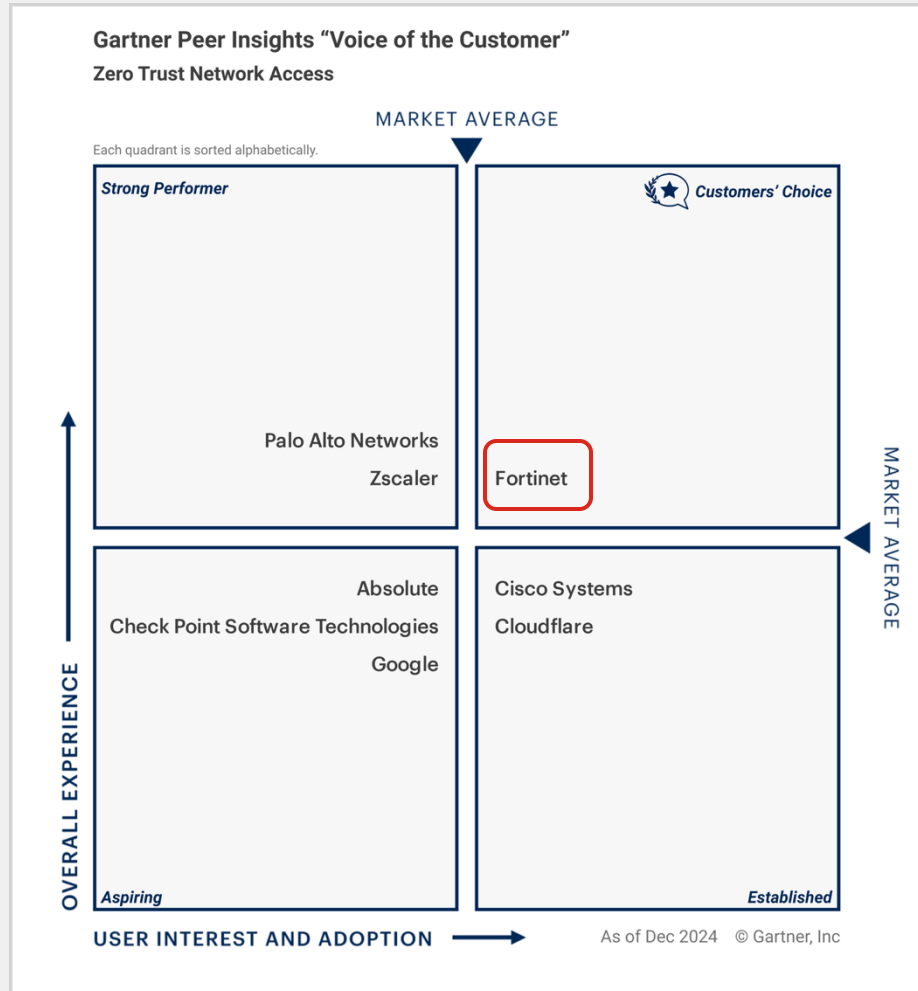
Open Ecosystem

- 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



2025 Gartner Peer Insights ZTNA

Fortinet став вибором користувачів в 2025 Gartner Peer Insights



Gartner.

“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



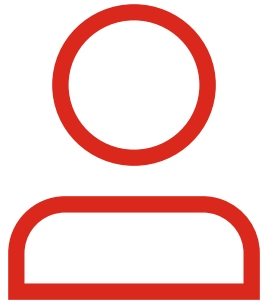


З чого починається ZTNA



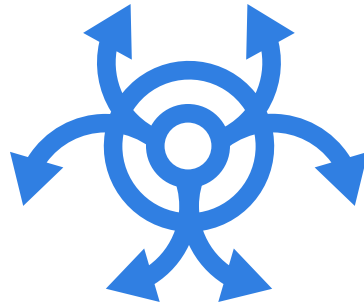
BYOD та віддалена робота стала буденністю

Робота звідусіль



- Збільшення векторів атак
- Вразливості ПК

Цільові атаки



- Профільні угруповання
- Проникнення та розповсюдження

Хмарні та SaaS сервіси



- Захист інформації
- Моніторинг

ZTNA принципи

Ніколи не довіряй. Завжди перевіряй.



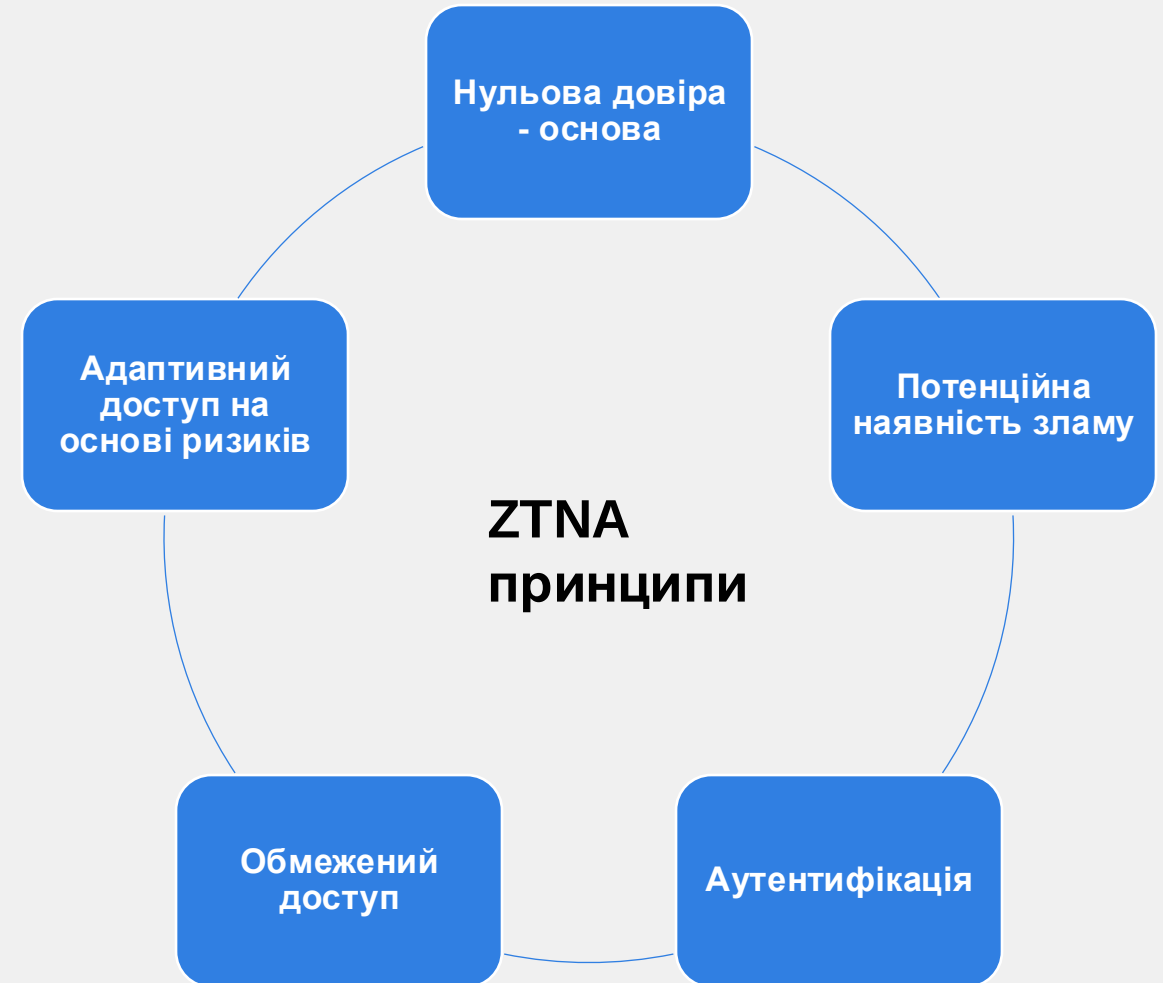
Надає доступ до мережі лише після автентифікації та авторизації особи



Обмежує доступ до мережі лише необхідними ресурсами/додатками



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



Джерело: Gartner

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

Перші кроки

З чого зазвичай починають?

Основа

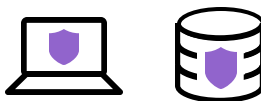
NGFW



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+)

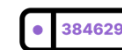


Опція

Другий фактор



FortiAuthenticator



FortiToken



FortiTrust Identity

та сторонні ID провайдери в рамках Security Fabric

Для кого?

Офісні співробітники нарівні з віддаленими

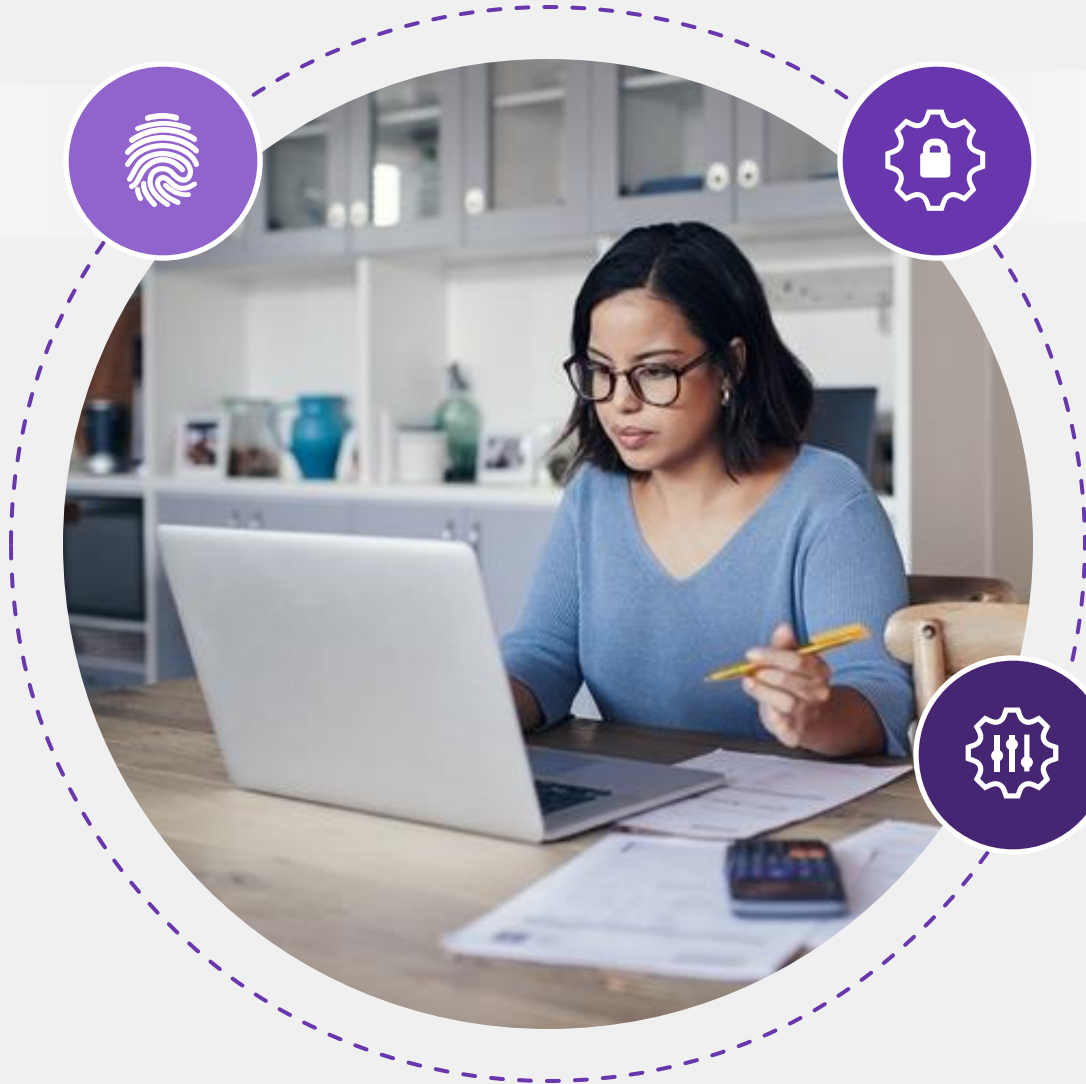
Перевірка кожної сесії

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

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

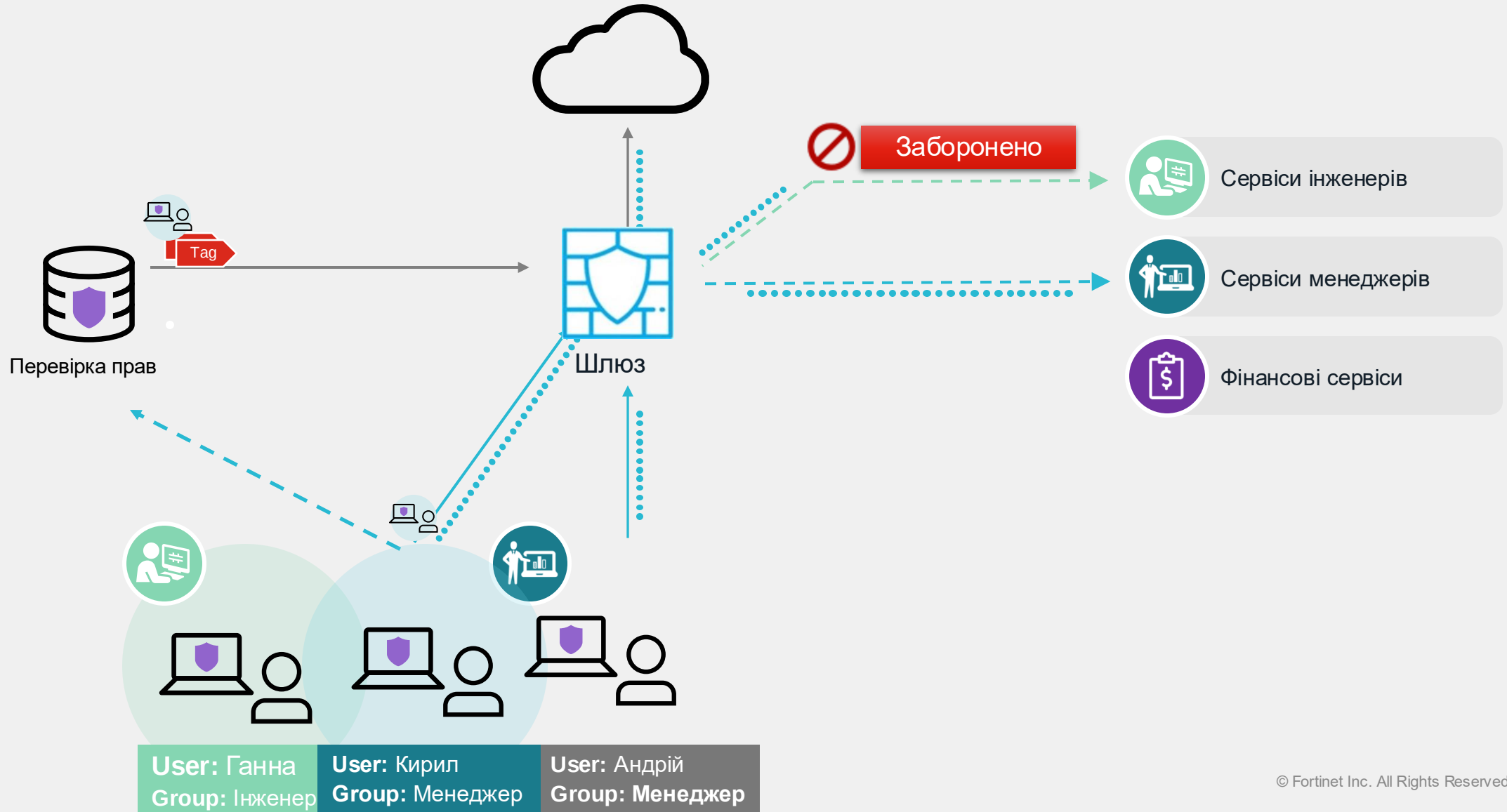
Аутсорс. Працює з
власних пристроїв

Ганна



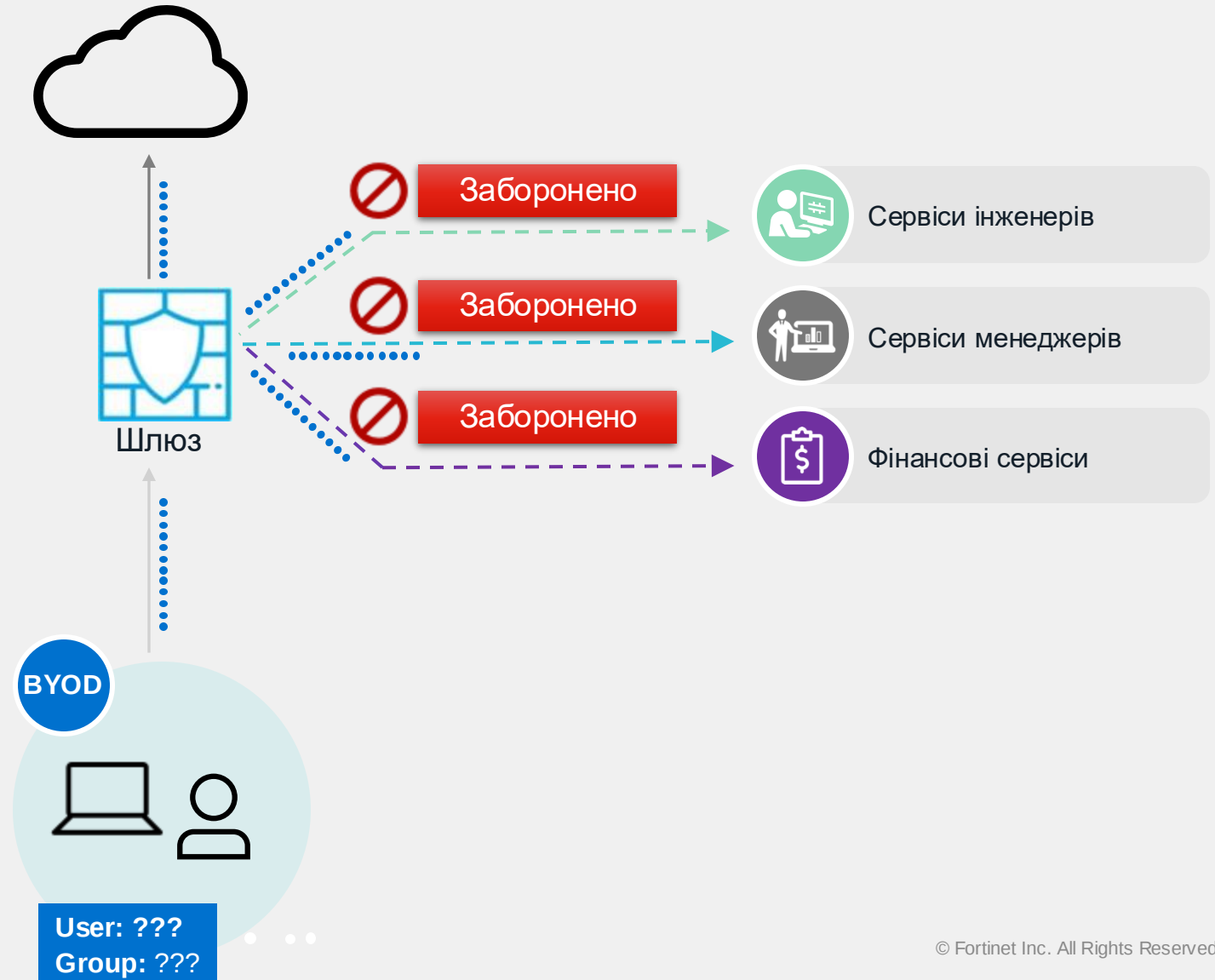
Розподілення доступу

На основі прав



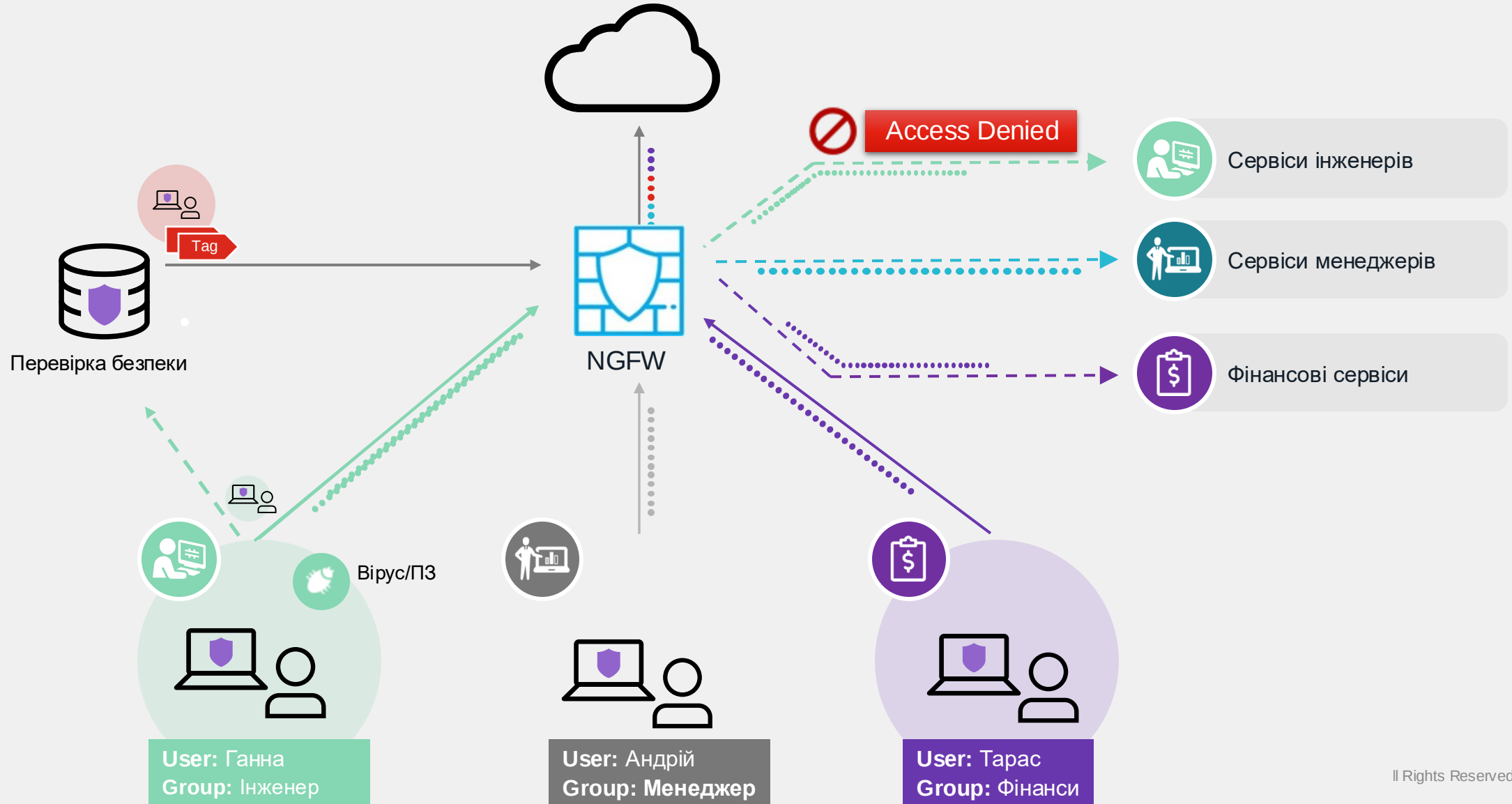
Робота з іншого ПК

Неперевірений ПК

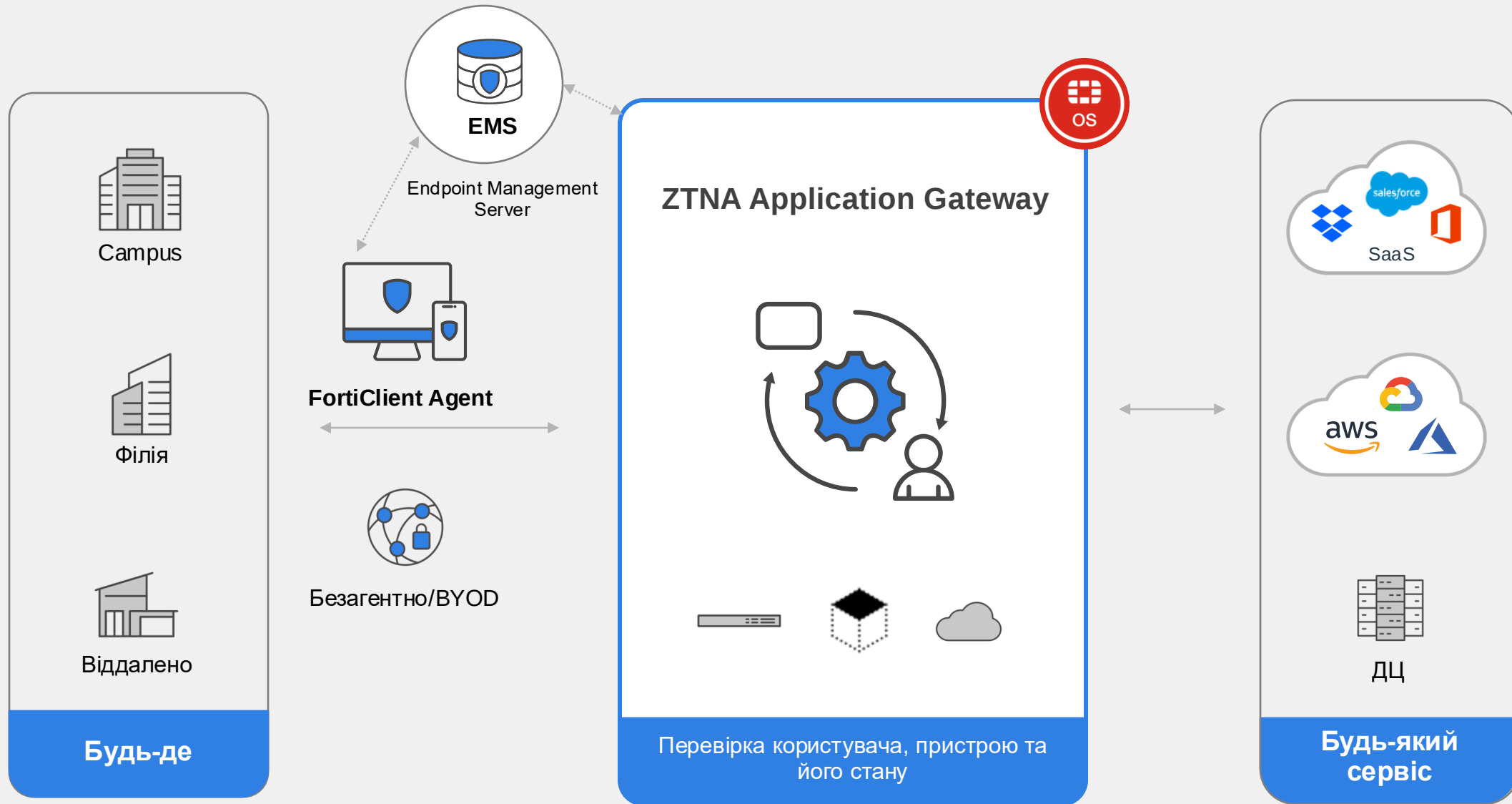


Блокування зараженого пристрою

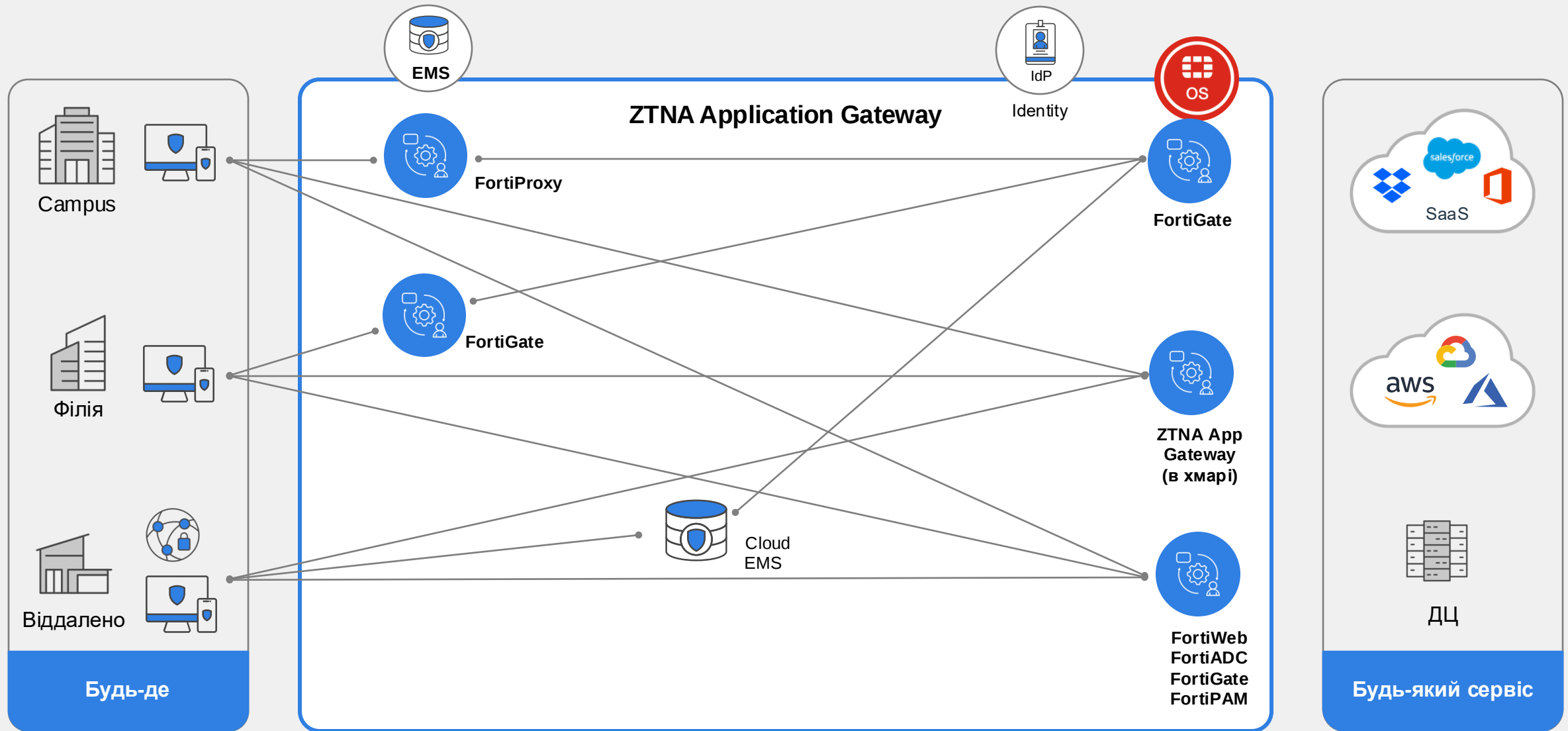
Або коли користувач «підхопив вірус»



Універсальне ZTNA рішення



Універсальне ZTNA рішення

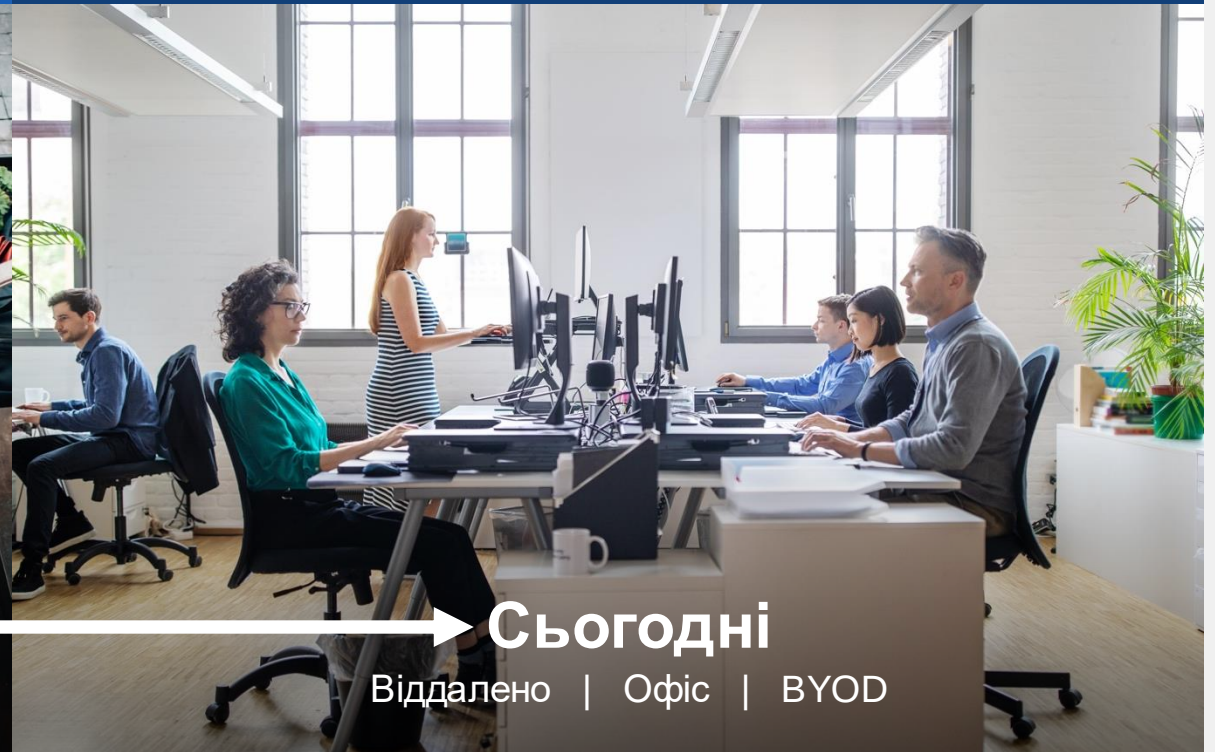


Еволюція ZTNA

ZTNA



Універсальний ZTNA



Перевод політик на ZTNA Tags

Етап 1

FortiGate-VM64-KVM

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Proxy Policy

Authentication Rules

Addresses

ZTNA

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

WiFi Controller

System

Security Fabric

Log & Report

Fortinet v7.4.1

16 Secu

Edit Policy

Name: ZTNA-Access

Type: Standard ZTNA

Incoming Interface: WAN (port3)

Source: all, ztna-saml-users

ZTNA Tag: ZTNA IP, Group-Domain-Users

ZTNA Server: ZTNA-webserver

Schedule: always

Action: ACCEPT, DENY

Firewall/Network Options

Protocol Options: PROT default

Security Profiles

AntiVirus: ☐

Web Filter: ☐

Video Filter: ☐

DNS Filter: ☐

Application Control: ☐

IPS: ☐

Select Entries

Search

ZTNA TAG (9)

EMS1 - IP (3)

ZTNA IP: all_registered_clients, Critical-Vulnerability, Group-Domain-Users

EMS1 - MAC (3)

ZTNA MAC: all_registered_clients, Critical-Vulnerability, Group-Domain-Users

IP (3)

LOCAL TAG: EMS_ALL_UNKNOWN_CLIEN, EMS_ALL_UNMANAGEABLE, FCTEMS_ALL_FORTICLOUD_S

Close

Statistics (since last reset)

ID	9
Last used	13 minute(s) ago
First used	2 hour(s) ago
Active sessions	1
Hit count	776
Total bytes	11.68 MB
Current bandwidth	0 bps

Clear Counters

Last 7 Days Bytes

SPU, Software

Additional Information

API Preview, References

OK, Cancel

- Оберіть один або кілька ZTNA tags
- З підтримкою безпеки



Вибір правил перевірки на основі одного чи кількох критеріїв

Edit Rule

OS: **Windows** | Mac | Linux | iOS | Android

Rule Type: **✓ User in AD Group**

Evaluate on FortiClient

AD Group

This rule applies to devices whose currently logged-in users are members of the selected AD Group. The rule does not consider computers' membership in that group.

AntiVirus Software
Certificate
EMS Management
File
IP Range
Logged in Domain
On-Fabric Status
OS Version
Registry Key
Running Process
Sandbox Detection
User Identity
Vulnerable Devices
Windows Security
Common Vulnerabilities and Exposures
Firewall Threat
FortiEDR

+

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

Edit Proxy Policy

Name: ZTNA-SaaS-Access

Type: Explicit Web | Transparent Web | FTP | **ZTNA**

Incoming Interface: WAN (port3)

Source: all

ZTNA Tag: ZTNA IP Group-Domain-Users

Destination: Webserver1

ZTNA Server: ZTNA-SaaS-Access-Proxy

Schedule: always

Action: **ACCEPT** | DENY

Security Profiles

- AntiVirus: **AV** default
- Web Filter: **WEB** default
- Application Control: **APP** default
- IPS: **IPS** default
- File Filter: **FILE** default
- DLP Profile: **DLP** Compliance-Credit-Cards
- SSL Inspection: **SSL** custom-deep-inspection

Select Entries

Search

ZTNA TAG (9)

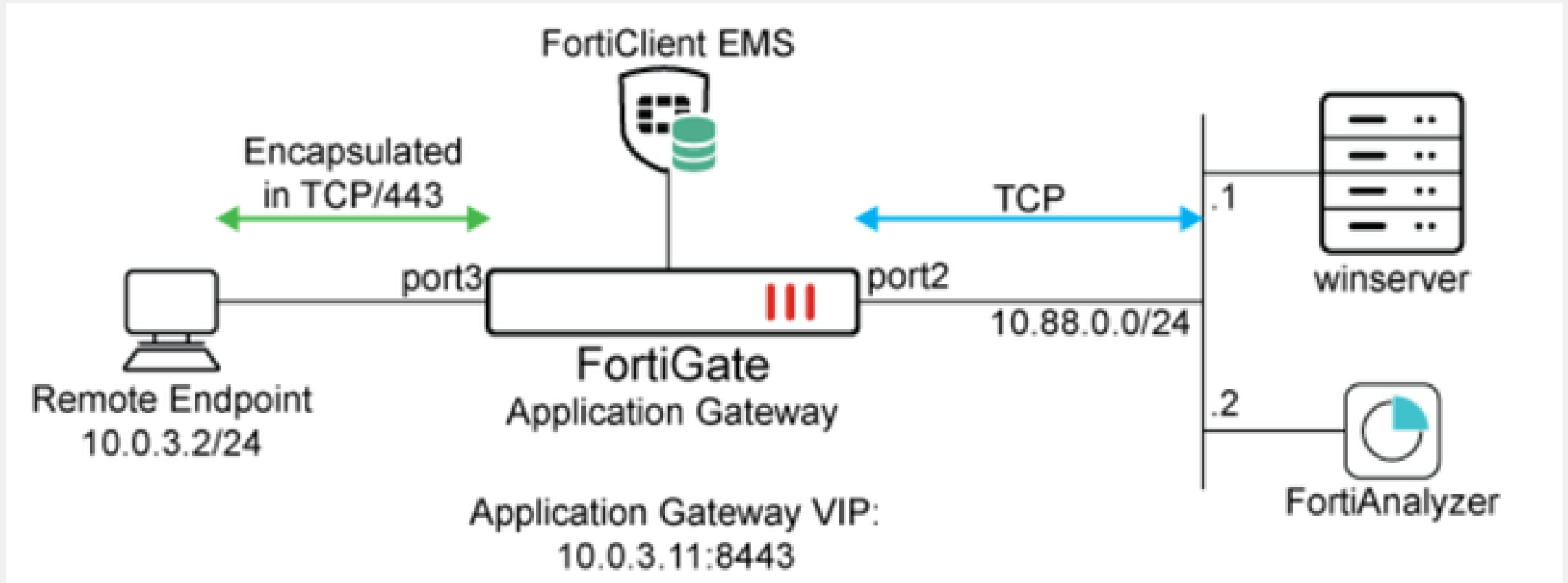
- EMS1 - IP (3)
 - ZTNA IP** all_registered_clients
 - ZTNA IP** Critical-Vulnerability
 - ZTNA IP** Group-Domain-Users
- EMS1 - MAC (3)
 - ZTNA MAC** all_registered_clients
 - ZTNA MAC** Critical-Vulnerability
 - ZTNA MAC** Group-Domain-Users
- IP (3)
 - LOCAL TAG EMS_ALL_UNKNOWN_CLIEN
 - LOCAL TAG EMS_ALL_UNMANAGEABLE
 - LOCAL TAG FCTEMS_ALL_FORTICLOUD

Close

OK Cancel

- Поступове увімкнення безпеки
- В першу чергу критичні сервіси

Доступ без VPN (ZTNA destination)



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



Доступ без VPN (ZTNA destination)

The screenshot displays the FortiClient -- Zero Trust Fabric Agent interface. On the left, a sidebar contains navigation icons for ZERO TRUST TELEMETRY, REMOTE ACCESS, ZTNA DESTINATION, VULNERABILITY SCAN, Notifications, Settings, and About. The main window is divided into two panes. The left pane shows the 'Create ZTNA Destination' dialog box with the following configuration:

- ZTNA Destination Configuration**
- Destination Name: SSH-FAZ
- Destination Host: 10.88.0.2:22
- Proxy Gateway: 10.0.3.11:8443
- Mode: Transparent (dropdown)
- ☐ Encryption
- ☐ Use external browser as user-agent for saml user authentication
- Buttons: Create, Cancel

The right pane shows the 'FortiZTNA Connection' window with the title 'ZTNA Destination'. It includes buttons for 'Add Destination' and 'Disable ZTNA'. Below these, three connection entries are listed, each with a red 'X' icon indicating a failed connection:

- SMB-winsrv**
Destination Host: 10.88.0.1:445
Proxy Gateway: 10.0.3.11:8443
Encryption: Yes
- RDP-winsrv**
Destination Host: 10.88.0.1:3389
Proxy Gateway: 10.0.3.11:8443
Encryption: No
- SSH-FAZ**
Destination Host: 10.88.0.2:22
Proxy Gateway: 10.0.3.11:8443
Encryption: No

Доступ без VPN ZTNA destination

New ZTNA Server

Settings Info

Type ⓘ IPv4

Name ZTNA-server

Comments

Connect On

Interface WAN (port3)

IP address 10.0.3.10

Port 9443

☒ SAML

Services and Servers

Default certificate ztna-wildcard

Service/server mapping

+ Create new Edit Delete

☐	Service	URL	Server	Type
No results				

OK Cancel

New Service/Server Mapping

Type ⓘ IPv4 IPv6

Service HTTP HTTPS SaaS (CASB) TCP Forwarding

Virtual Host Any Host Specify

Match by Substring Wildcard

Host www.example1.com

Use certificate Fortinet_CA_SSL

Match path by Substring Wildcard Regular Expression

Path map1

☒ Server

Address type IP FQDN

IP address 0.0.0.0

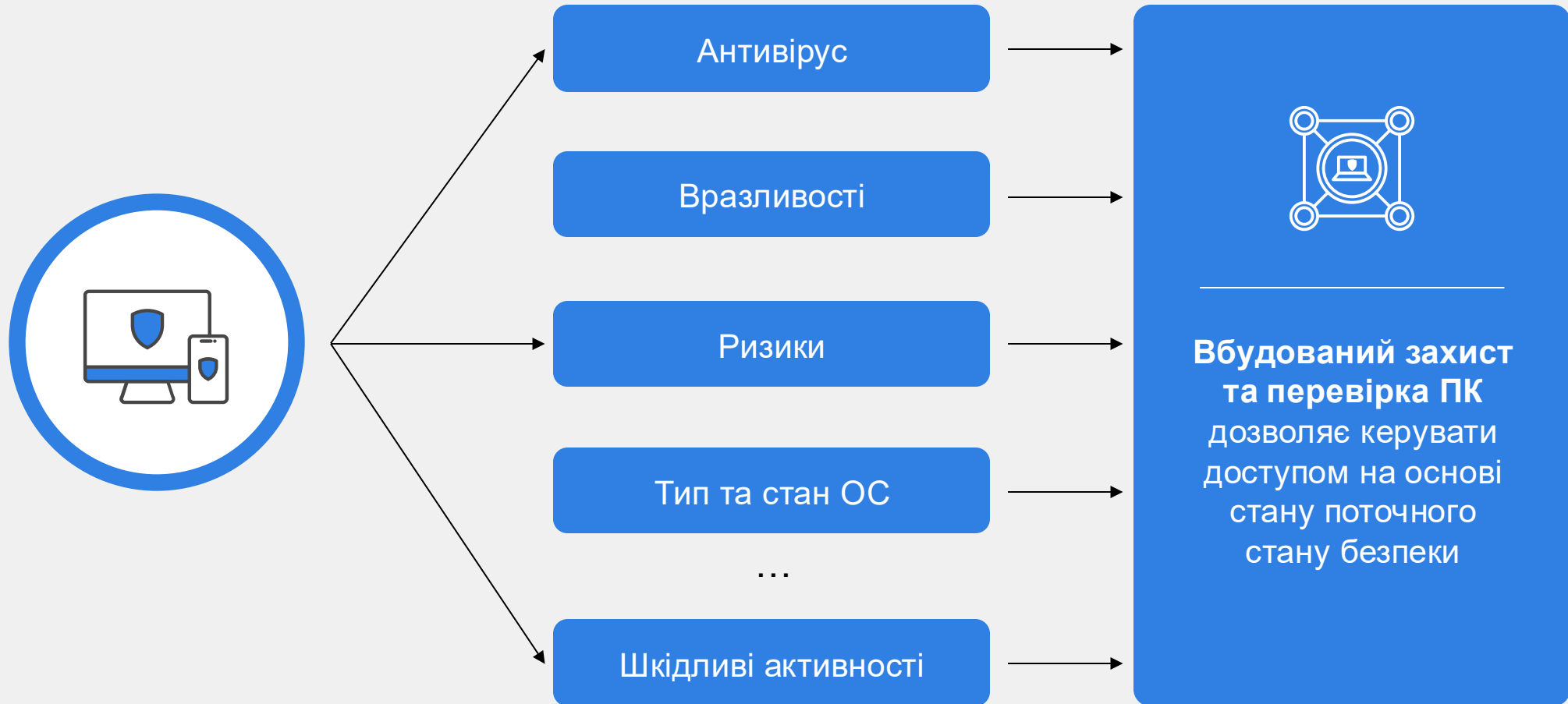
Port 443

OK Cancel



Інтегрована безпека що приймає участь в ZTNA

Постійна перевірка пристрою





← Critical Vulnerabilities Patch All

☆ ▾ Filter ▾ 🔍

Vulnerability Name ▾	FortiGuard ID ▾	CVE ID ▾	Category ▾	Affected Endpoints ▾	Patch Type ▾
Cumulative Security Update for Internet Explorer	1492	CVE-2016-0178	OS	3	<button>Patch</button>
Firefox SVG Animation Remote Code Execution	31801	CVE-2016-9079	Browser	3	<button>Patch</button>
Sandbox restrictions not applied to nested frame elements	26051	CVE-2016-3223	AntiVirus	2	<button>Patch</button>
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 Execution					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

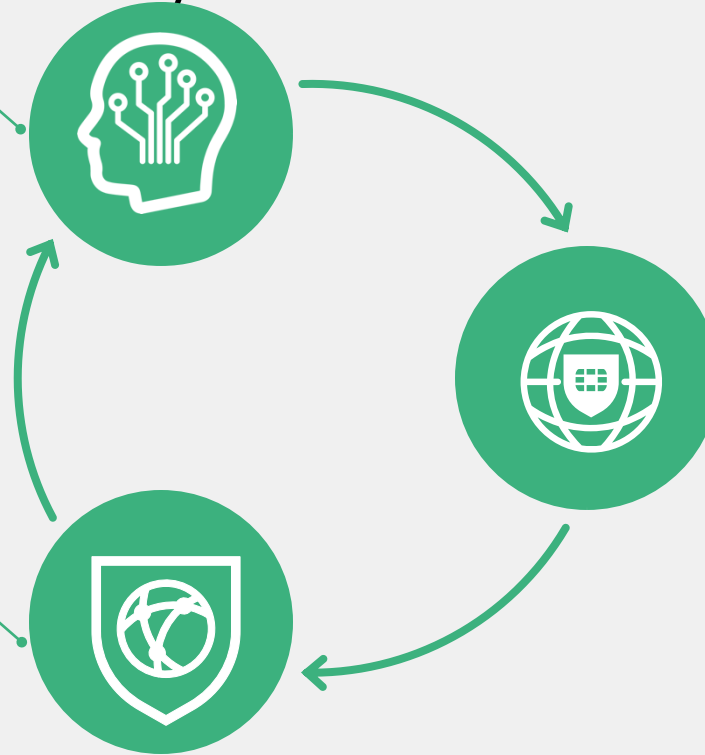
FortiGuard Web Filtering

Аналіз за допомогою штучного інтелекту

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

Захист в деталях

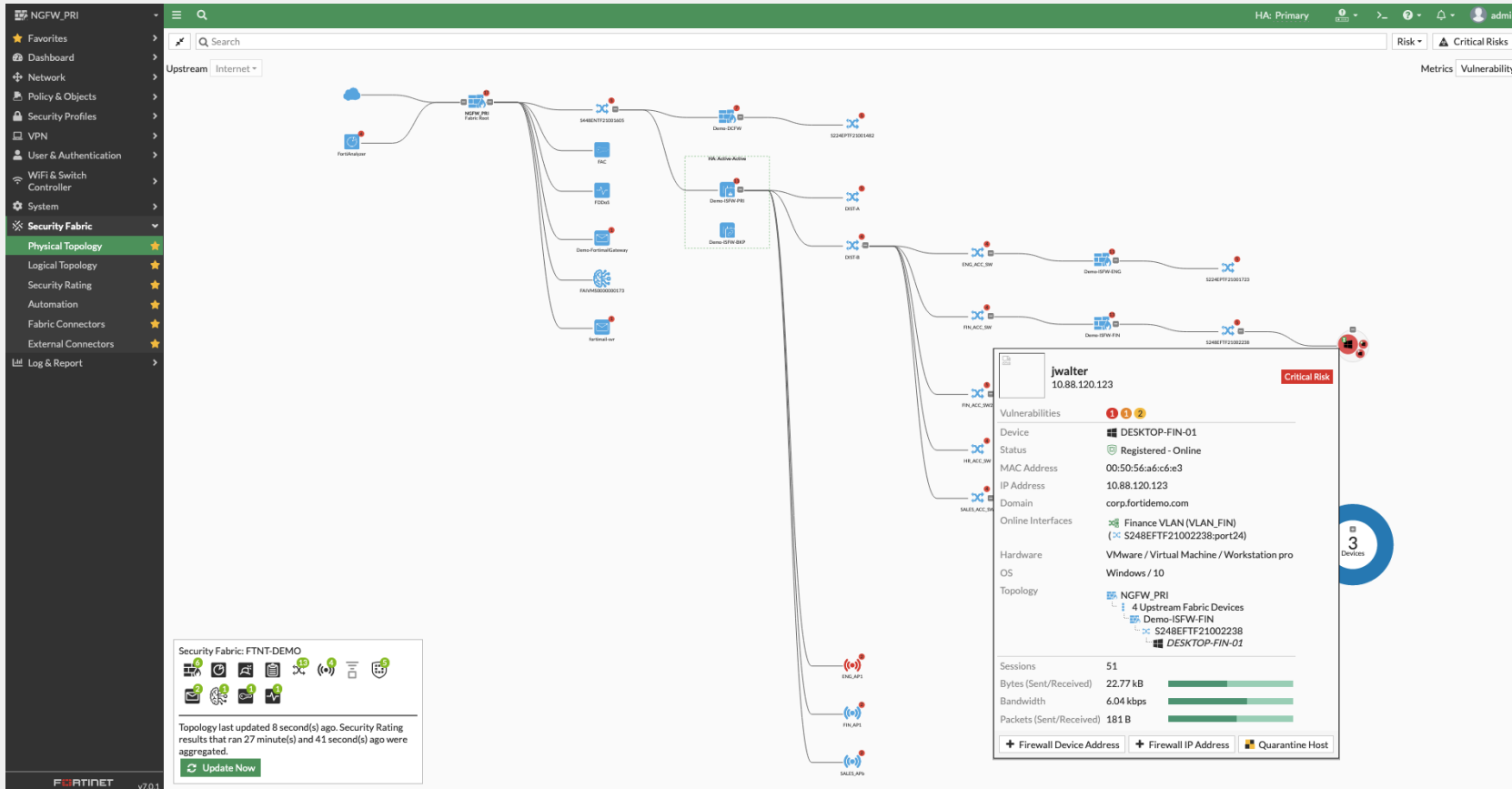
- Повний спектр веб-захисту від невідомих і відомих загроз
- Кілька рівнів захисту з майже нульовими помилковими результатами



Консистентні дані

- Мережеві пристрої, ПК та хмари
- Різні можливості розгортання

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

Впровадження ZTNA

Етап 1

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



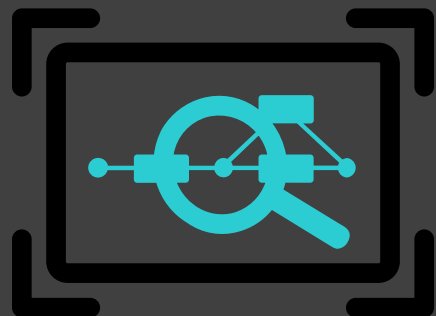
Етап 2

- 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



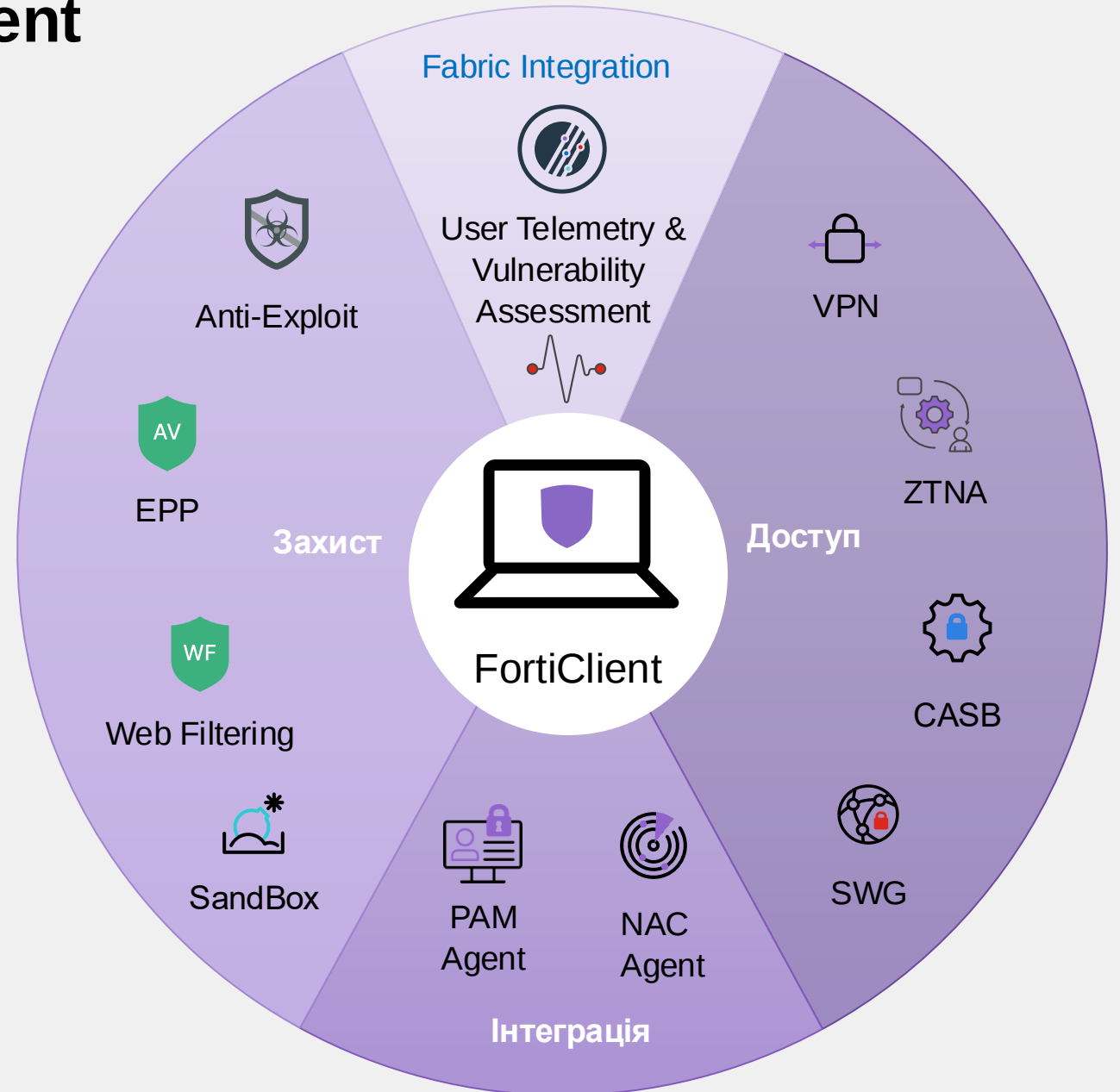
З чого починається EDR/XDR



Уніфікований агент - FortiClient

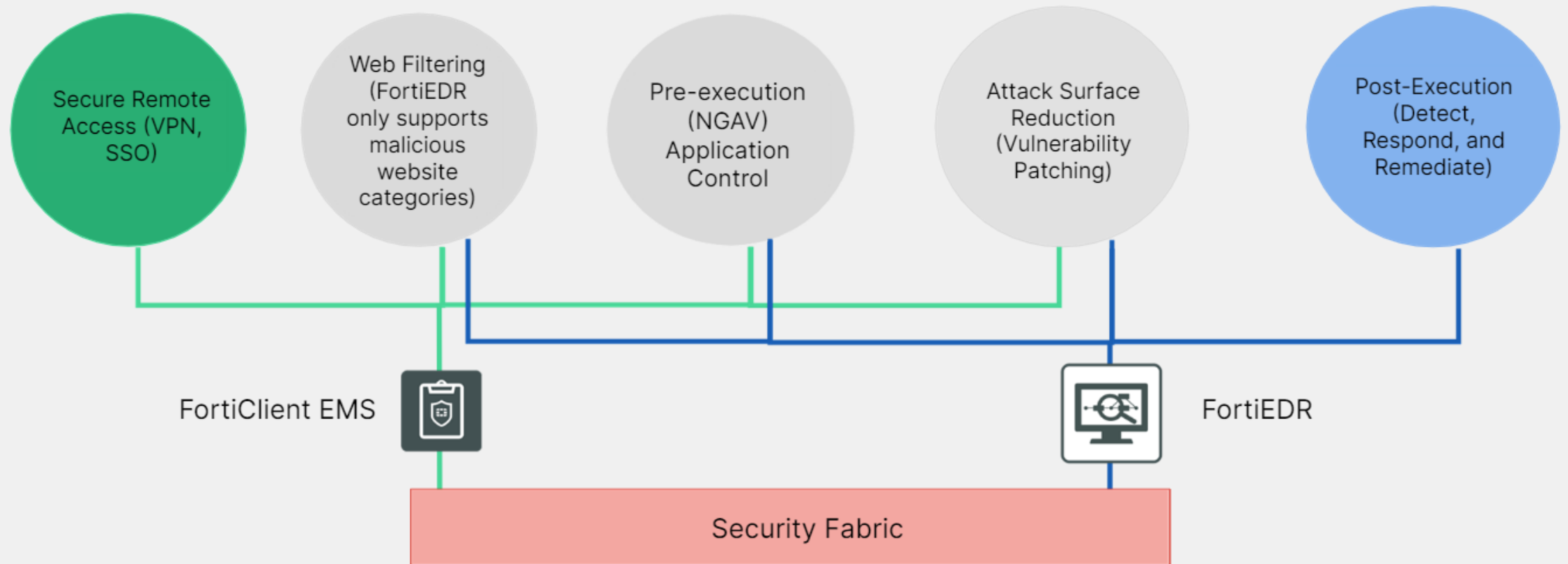
Один агент для всього*

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



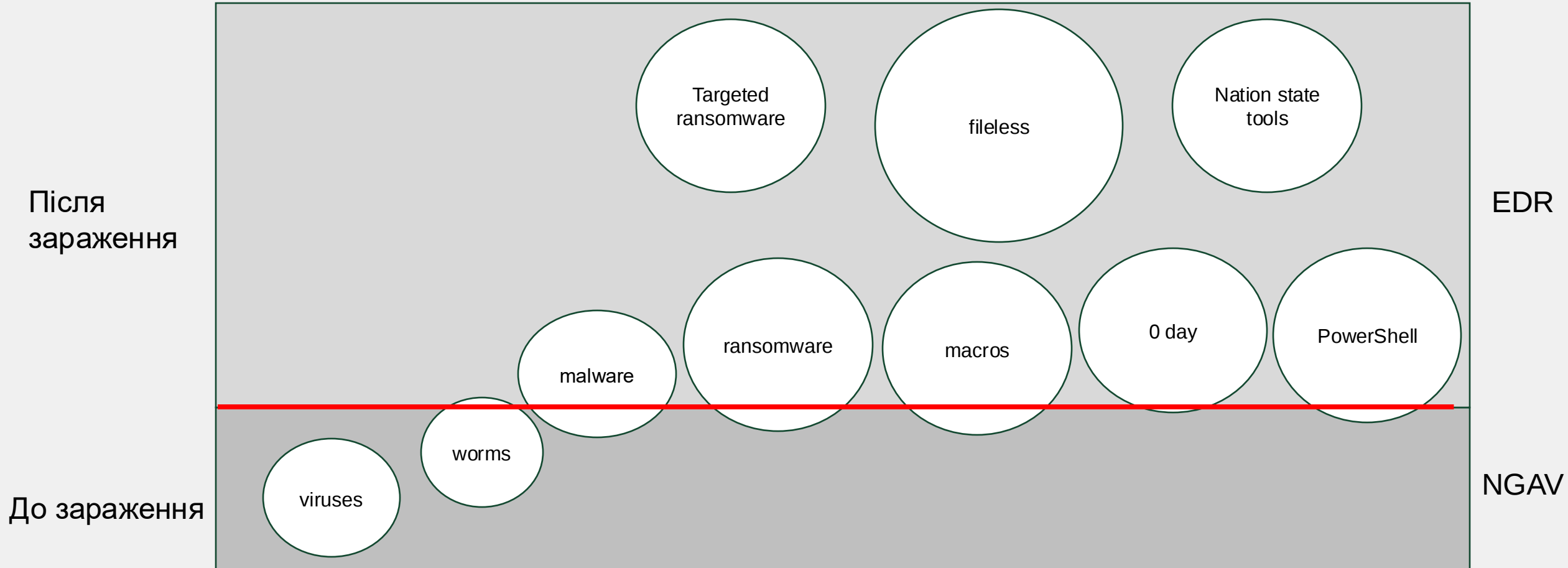
Набір функцій

FortiEDR це не тільки ПК співробітників



Детальніше щодо захисту

Від чого захищає EDR



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

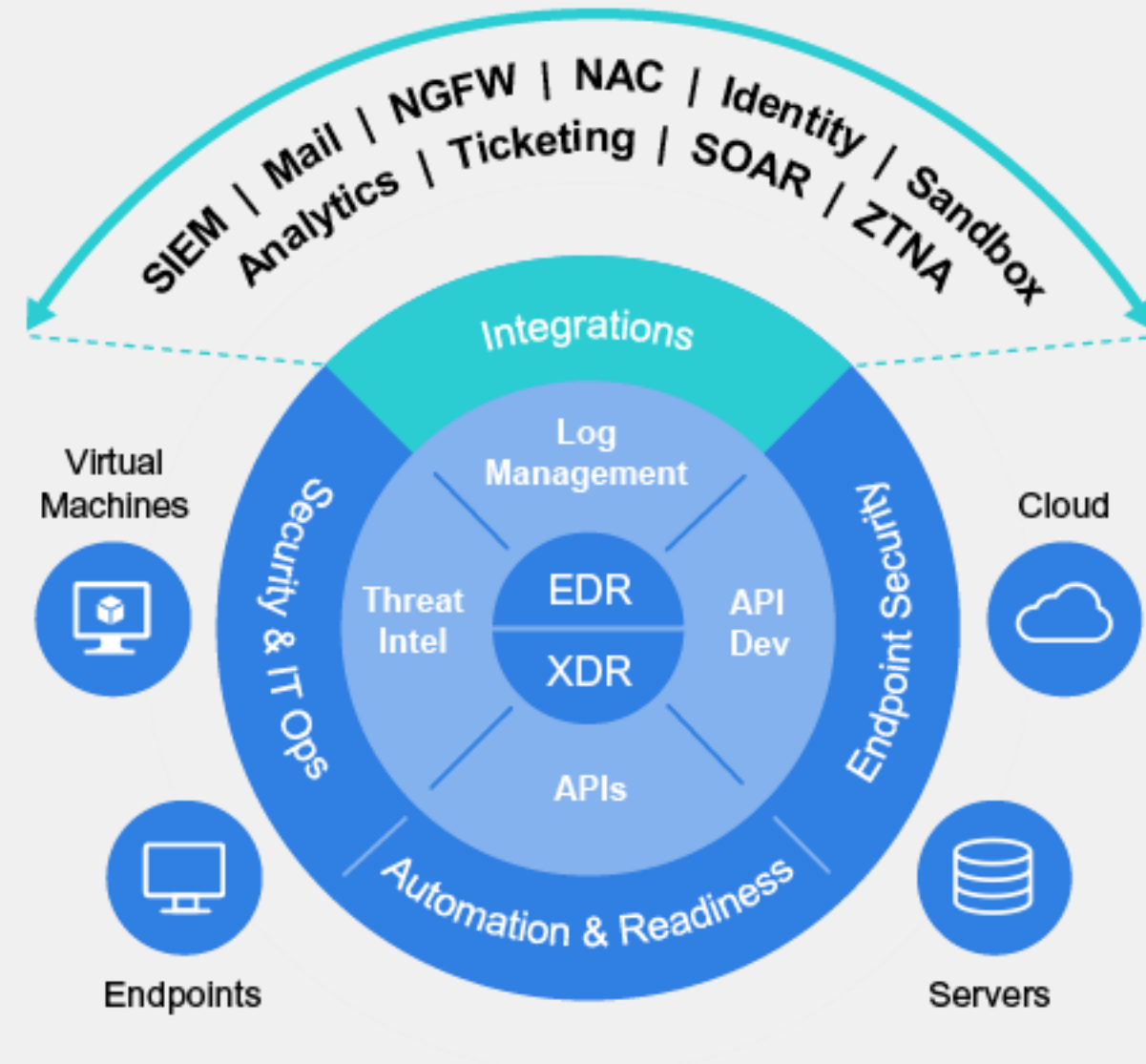


Основи FortiEDR

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

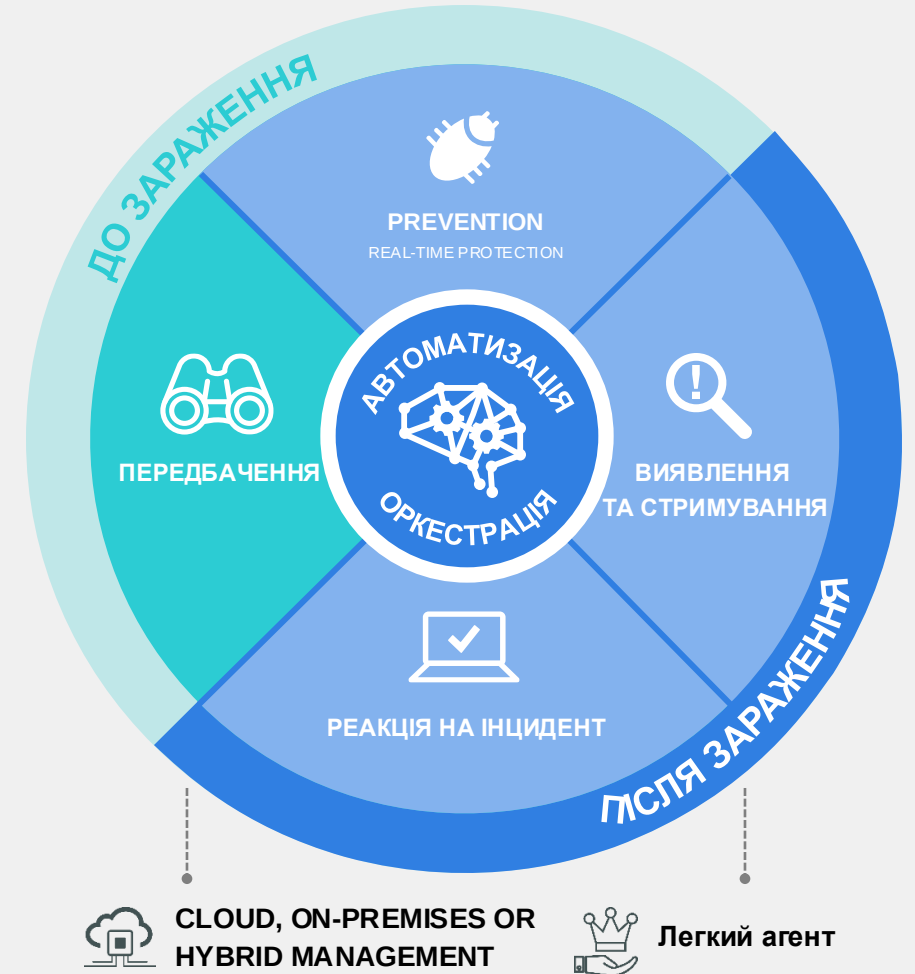


Проактивне зменшення площі атаки



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

DASHBOARD EVENT VIEWER 2004 FORENSICS COMMUNICATION CONTROL 119 SECURITY SETTINGS						
APPLICATIONS						
Unresolved Mark As... Delete Modify Action Advanced Filter Export						
APPLICATION	VENDOR	REPUTATION	VULNERABILITY	FIRST SEEN	LAST SEEN	
☒ Google Chrome	Signed Google		Critical	15-Oct-2020	08-Mar-2021	
☐ 86.0.4240.75			Critical	15-Oct-2020	16-Oct-2020	
☐ 86.0.4240.183		Unknown	Critical	03-Nov-2020	03-Nov-2020	
☐ 87.0.4280.66			Critical	01-Dec-2020	13-Jan-2021	
☐ 88.0.4324.104		Unknown	Critical	01-Feb-2021	03-Feb-2021	
☐ 87.0.4280.141			Critical	09-Feb-2021	02-Mar-2021	
☐ 88.0.4324.150		Unknown	Critical	11-Feb-2021	22-Feb-2021	
☐ 88.0.4324.146		Unknown	Critical	12-Feb-2021	19-Feb-2021	
☐ Pastebin Desktop	Unsigned Unknown Vendor		Unknown	16-Oct-2020	18-Oct-2020	



Профілактика

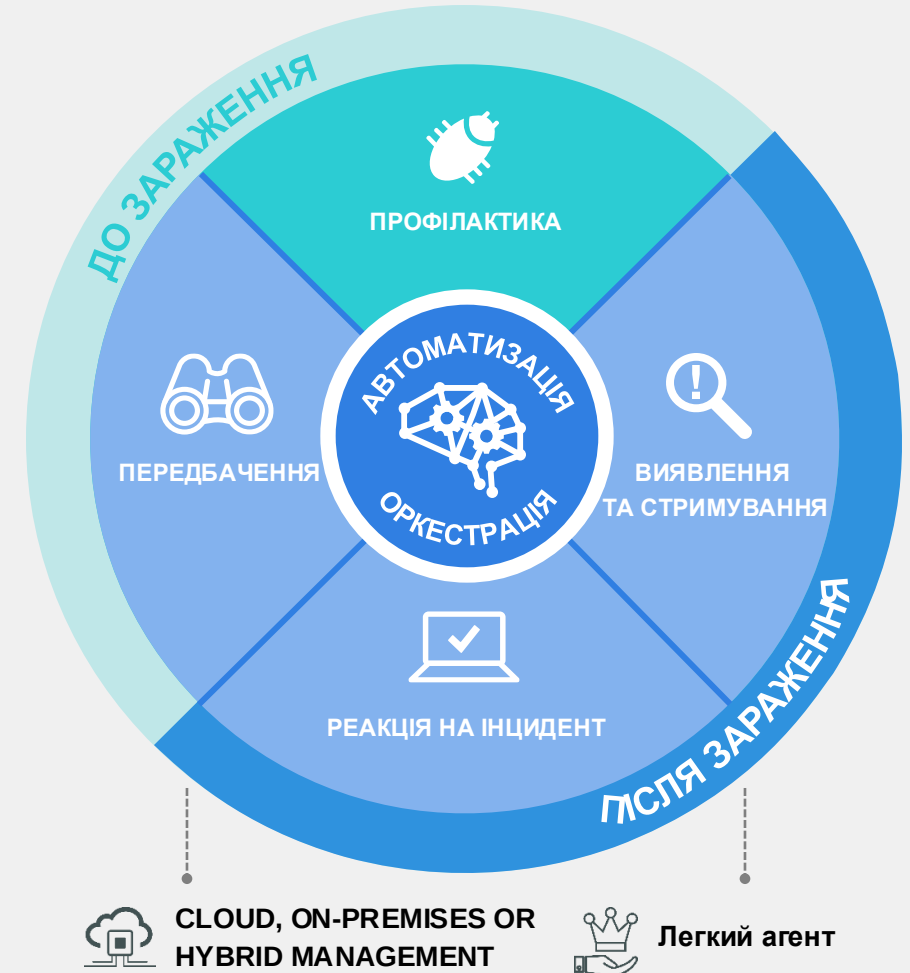


Протидія в реальному часі

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



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

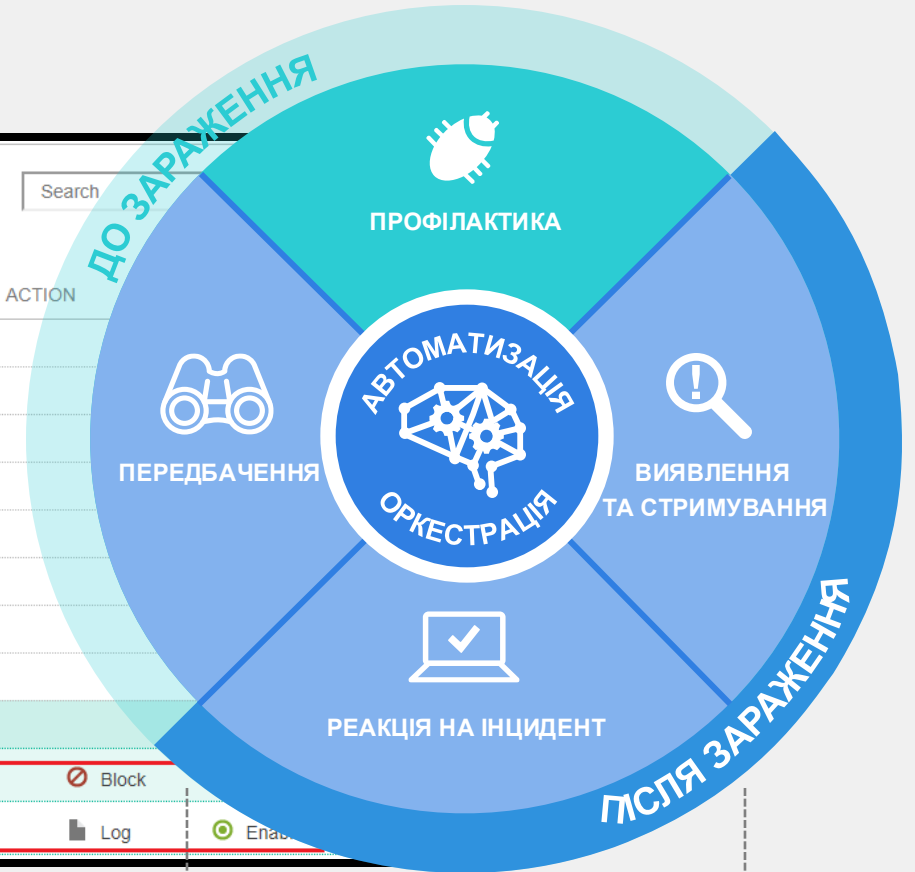


Вбудовані політики безпеки



- Захист з першої хвилини використання
- Оновлення за допомогою FortiGuard

SECURITY POLICIES					Search
Clone Policy Set Mode Assign Collector Group Delete					
☐	All	POLICY NAME	RULE	ACTION	
▶ ☐	Application Control	FORTINET	☐		
▶ ☐	Device Control	FORTINET	☐		
▶ ☐	Execution Prevention	FORTINET	☒		
▶ ☐	Exfiltration Prevention	FORTINET	☒		
▶ ☐	eXtended Detection	FORTINET	☐		
▶ ☐	Mobile Devices	FORTINET	☒		
▶ ☐	Ransomware Prevention	FORTINET	☒		
▶ ☐	AF mobile devices upda...		☒		
▼ ☐	Mobile Devices		☒		
				Malicious File Detected	☒ Block
				Malicious URL/IP Detected	☐ Log ☒ Enable



CLOUD, ON-PREMISES OR
HYBRID MANAGEMENT



Легкий агент



Виявлення та блокування

EVENTS							
All	Last 30 days	Archive	Mark As...	Export	Handle Event	Delete	Forensics
				System Defined	Search for events		
	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
☐	hobgoblin (7 events)						
☐	50671	hobgoblin	wermgr.exe	Inconclusive	File Creation	16-Mar-2023, 16:50:26	16-Mar-2023, 16:50:26
☐	50593	hobgoblin	explorer.exe	Suspicious	2 destinations	16-Mar-2023, 16:49:53	16-Mar-2023, 16:56:59
☐	50580	hobgoblin	mrxs_installer.exe	Suspicious	File Execution At...	16-Mar-2023, 16:49:43	16-Mar-2023, 16:57:46
☐	50662	hobgoblin	svchost.exe	Malicious	Modify OS Setti...	16-Mar-2023, 16:50:21	16-Mar-2023, 16:50:21
☐	50647	hobgoblin	net.exe	Malicious	10.20.10.9	16-Mar-2023, 16:50:08	16-Mar-2023, 16:50:08
☐	50634	hobgoblin	MSSVCCFG.dll	Malicious	Network Access	16-Mar-2023, 16:50:03	16-Mar-2023, 16:50:03
Process owner: None Certificate: Unsigned Process path: C:\Program Files\Windows NT\MSSVCCFG.dll Raw Data items: 1							
☐	50612	hobgoblin	msedge.exe	Malicious	Network Access	16-Mar-2023, 16:49:58	16-Mar-2023, 16:49:58

CLASSIFICATION DETAILS

Malicious Fortinet

Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

Automated analysis steps completed by Fortinet Details

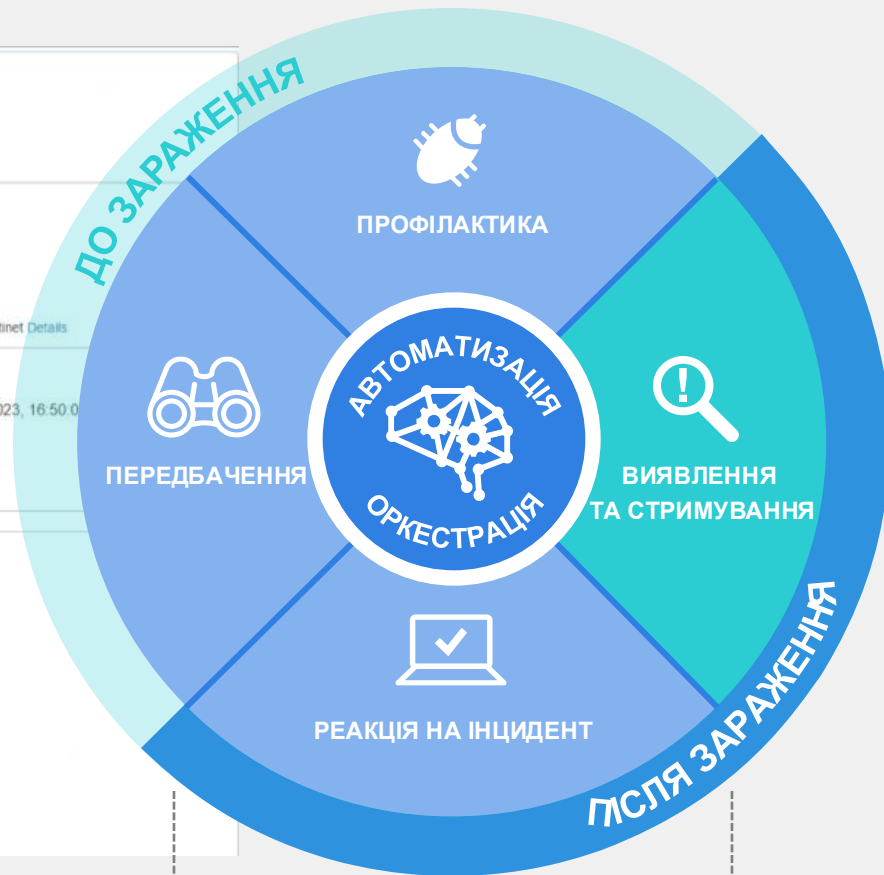
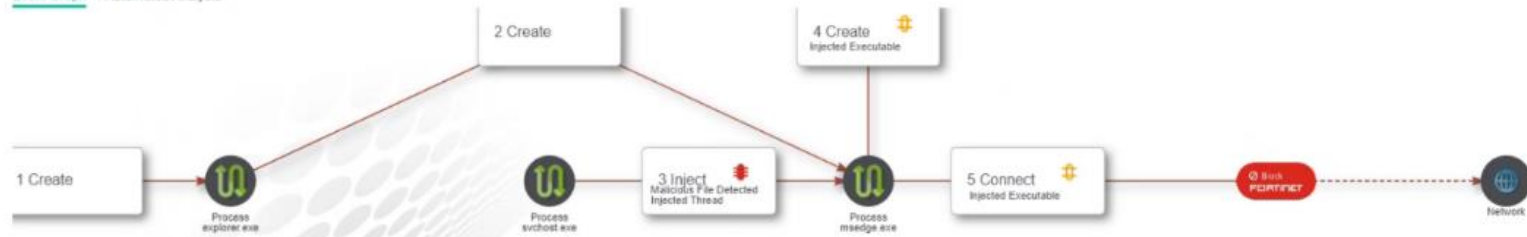
History

Malicious, by Fortinet, on 16-Mar-2023, 16:50:03

ADVANCED DATA

Event Graph

Automated Analysis



CLOUD, ON-PREMISES OR
HYBRID MANAGEMENT



Легкий агент



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

 **Malicious FORTINET**

Threat name: Kryptik.CTQltr
Threat family: W64
Threat type: Unknown

Automated analysis steps completed by Fortinet [Details](#)

History

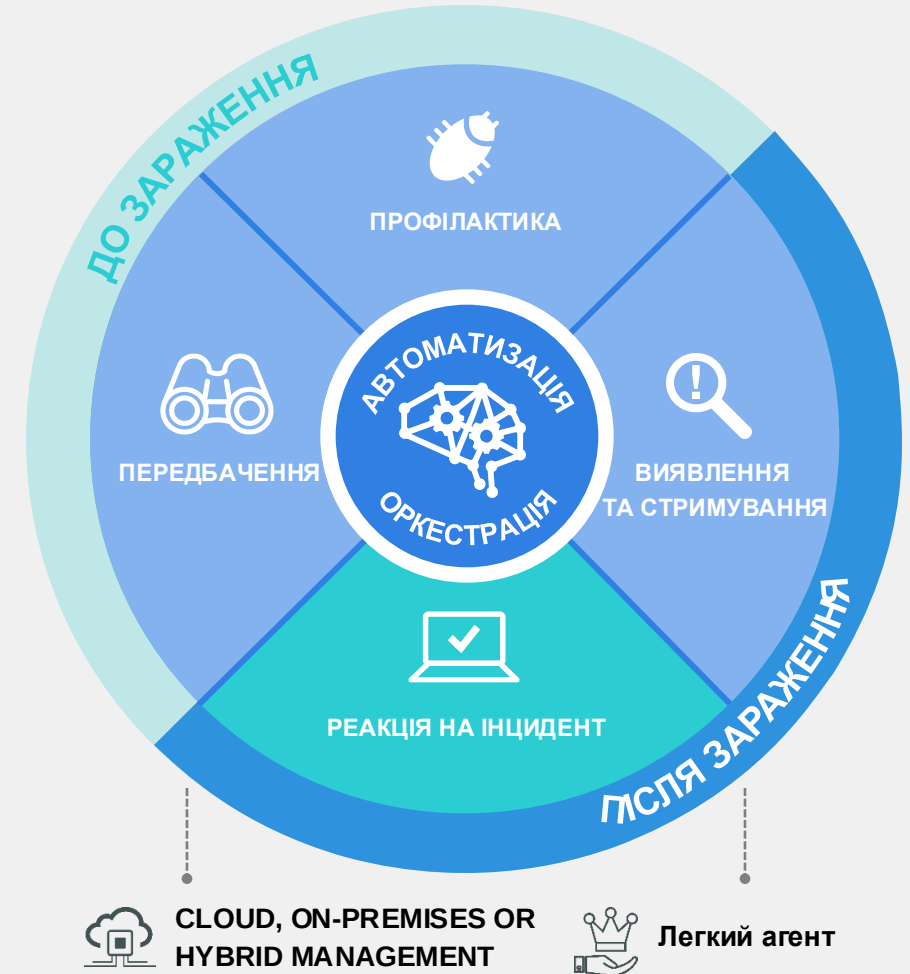
▼  Malicious, by FortinetCloudServices, on 30-Mar-2022, 01:06:47

- Device **DESKTOP-VM-BN** was isolated on NAC **TME-FortiNACz**
- Process **...esktop\Ayfaga3.exe** with PID **2572** was terminated at device **DESKTOP-VM-BN** 4 times
- File **...esktop\Ayfaga3.exe** was deleted on device **DESKTOP-VM-BN** 2 times
- IP **104.168.44.45** was added to malicious IP addresses on firewall **FortiGate**

Triggered Rules

▼  G3 Exfiltration Prevention clone

- ▷  Malicious File Detected
- ▷  Tampered Executable - Critical Executable was Tampered With

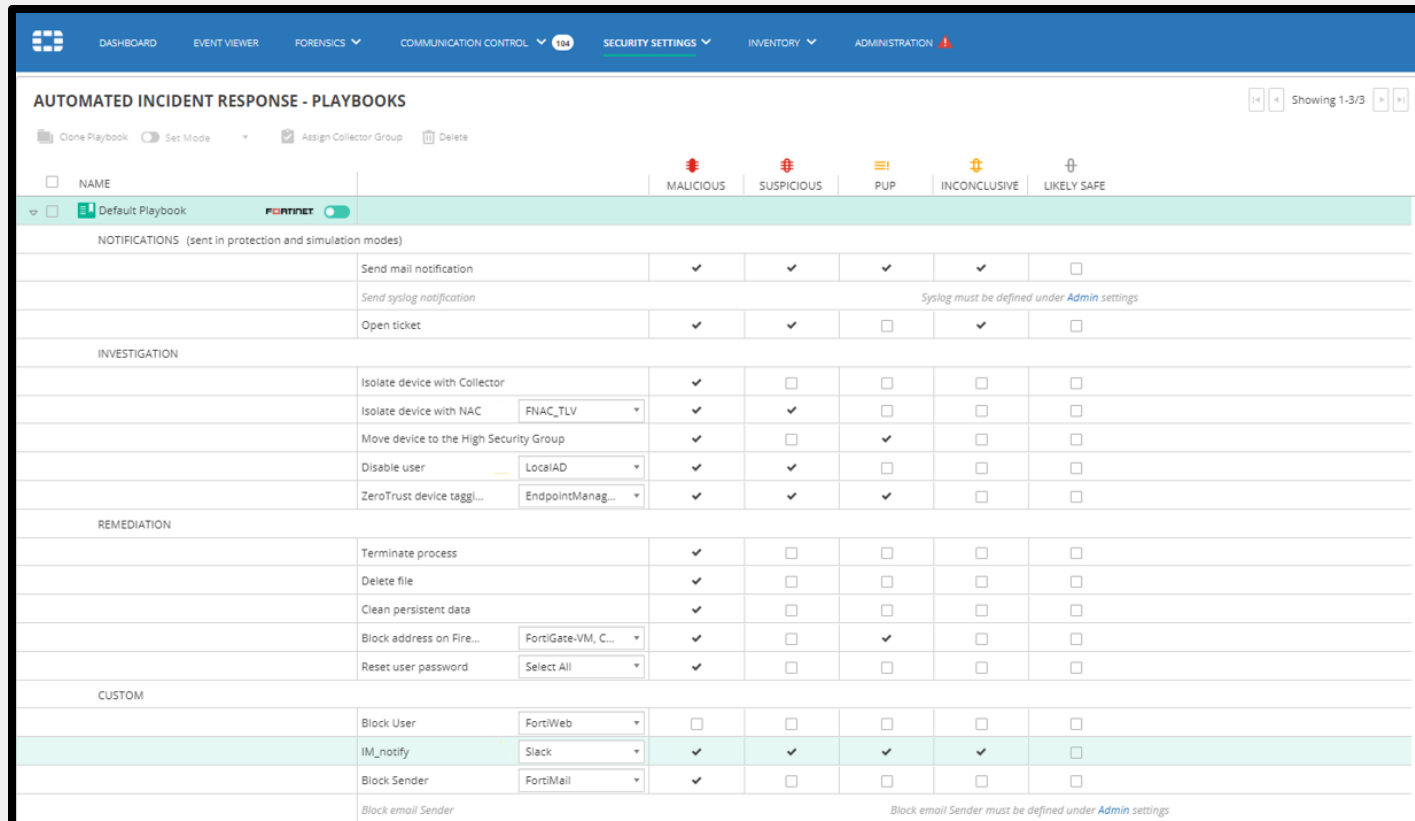


Різні реакції на різні рівні критичності

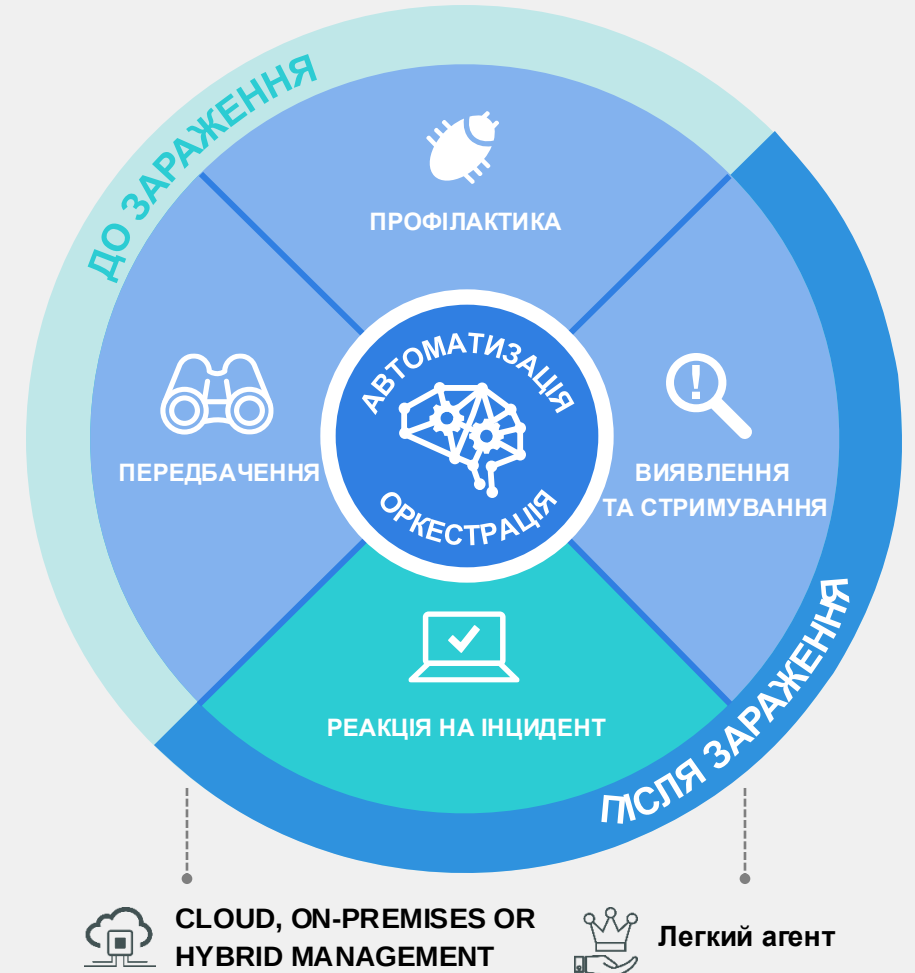
Різні playbooks для різного рівня загроз

Налаштування сповіщень та протидії

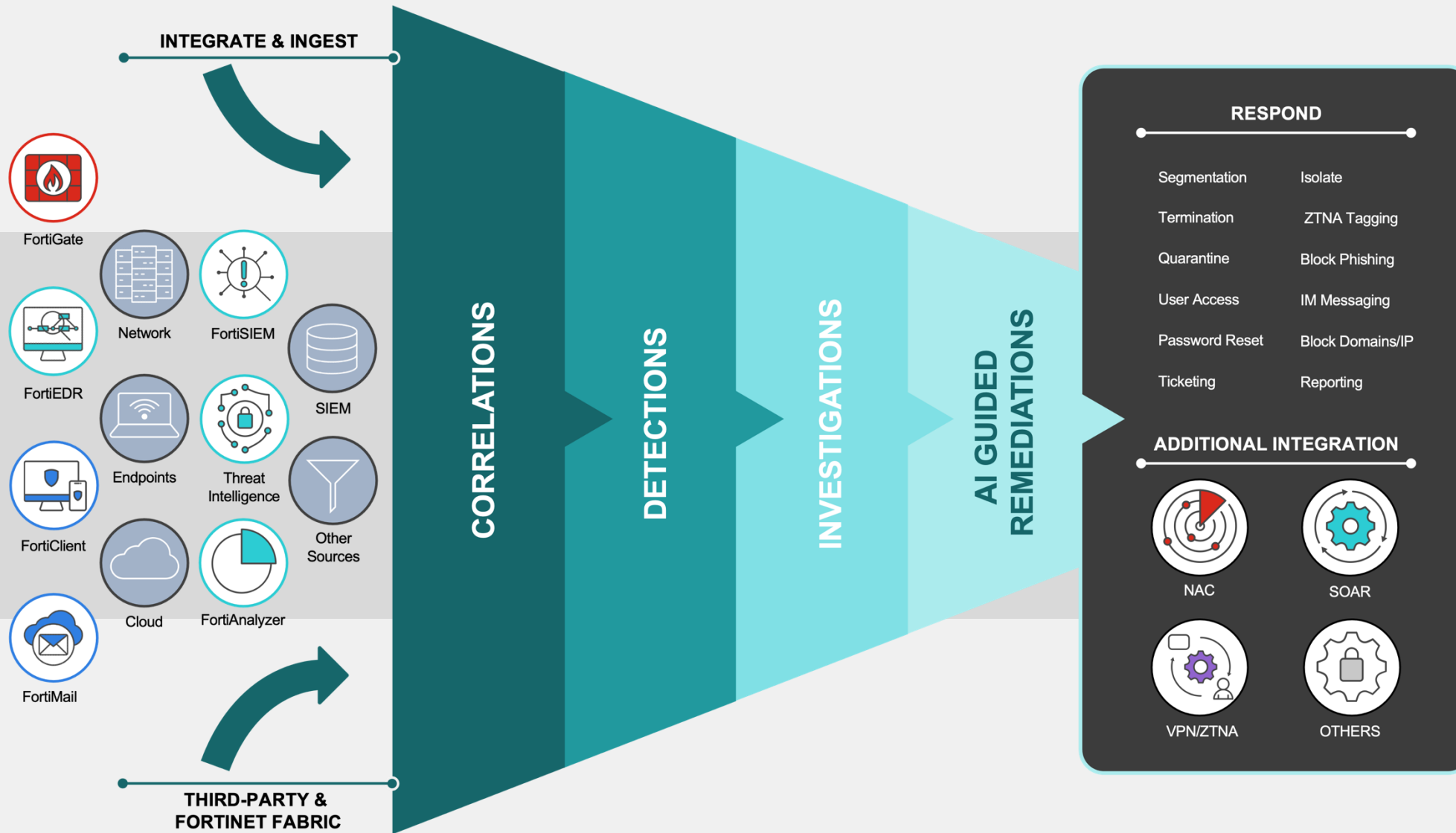
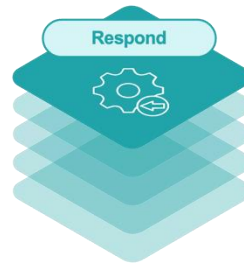
Протидія за допомогою як інструментів Fortinet так і сторонніх



NAME	MALICIOUS	SUSPICIOUS	PUP	INCONCLUSIVE	LIKELY SAFE
NOTIFICATIONS (sent in protection and simulation modes)					
Send mail notification	✓	✓	✓	✓	□
Send syslog notification				Syslog must be defined under Admin settings	
Open ticket	✓	✓	□	✓	□
INVESTIGATION					
Isolate device with Collector	✓	□	□	□	□
Isolate device with NAC	FNAC_TLV	✓	□	□	□
Move device to the High Security Group	✓	□	✓	□	□
Disable user	LocalAD	✓	□	□	□
ZeroTrust device tagg...	EndpointManag...	✓	✓	✓	□
REMEDIATION					
Terminate process	✓	□	□	□	□
Delete file	✓	□	□	□	□
Clean persistent data	✓	□	□	□	□
Block address on Fire...	FortiGate-VM, C...	✓	□	✓	□
Reset user password	Select All	✓	□	□	□
CUSTOM					
Block User	FortiWeb	□	□	□	□
IM_notify	Slack	✓	✓	✓	□
Block Sender	FortiMail	✓	□	□	□
Block email Sender					



В чому відмінність EDR від XDR



Ліцензування FortiEndpoint

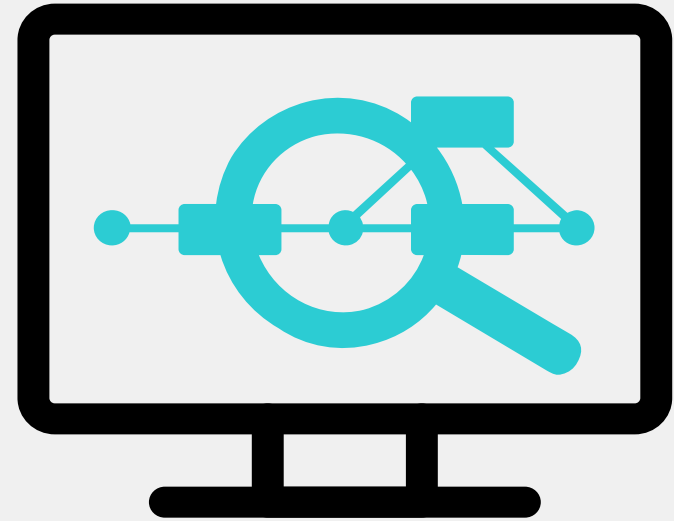


FortiEndpoint



FortiClient

+

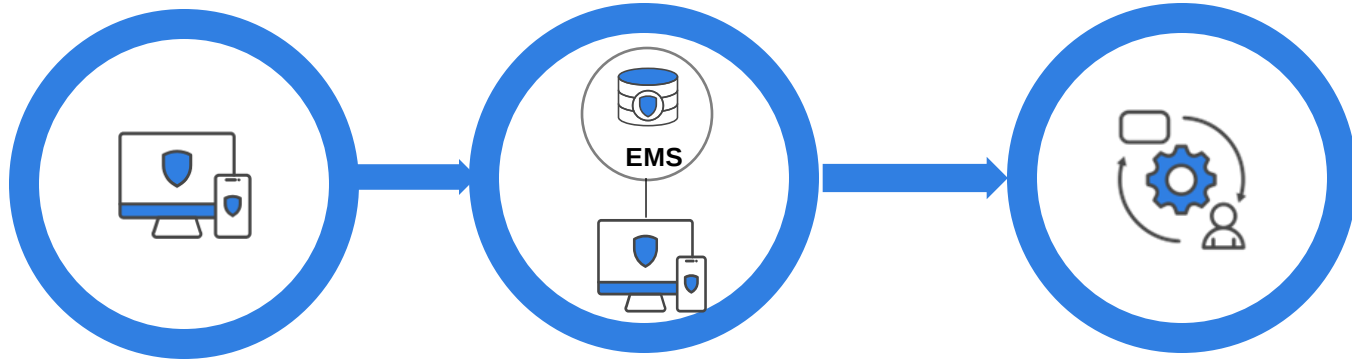


FortiXDR

Уніфікований агент

Постійні інновації і 20М інстальованих агентів

Безпечний доступ



FortiClient VPN

- Традиційний VPN
- Free FortiClient

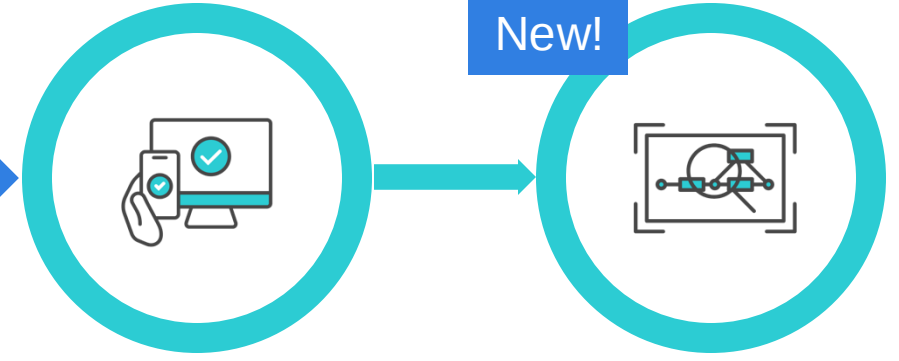
Видимість ПК (SaaS / On-prem)

- 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



Формфактори FortiEndpoint



Апаратні
рішення

- Perpetual



Віртуальні машини

- Perpetual
- Subscription



Public Clouds

- BYOL
 - Perpetual
 - Subscription
- PAYG



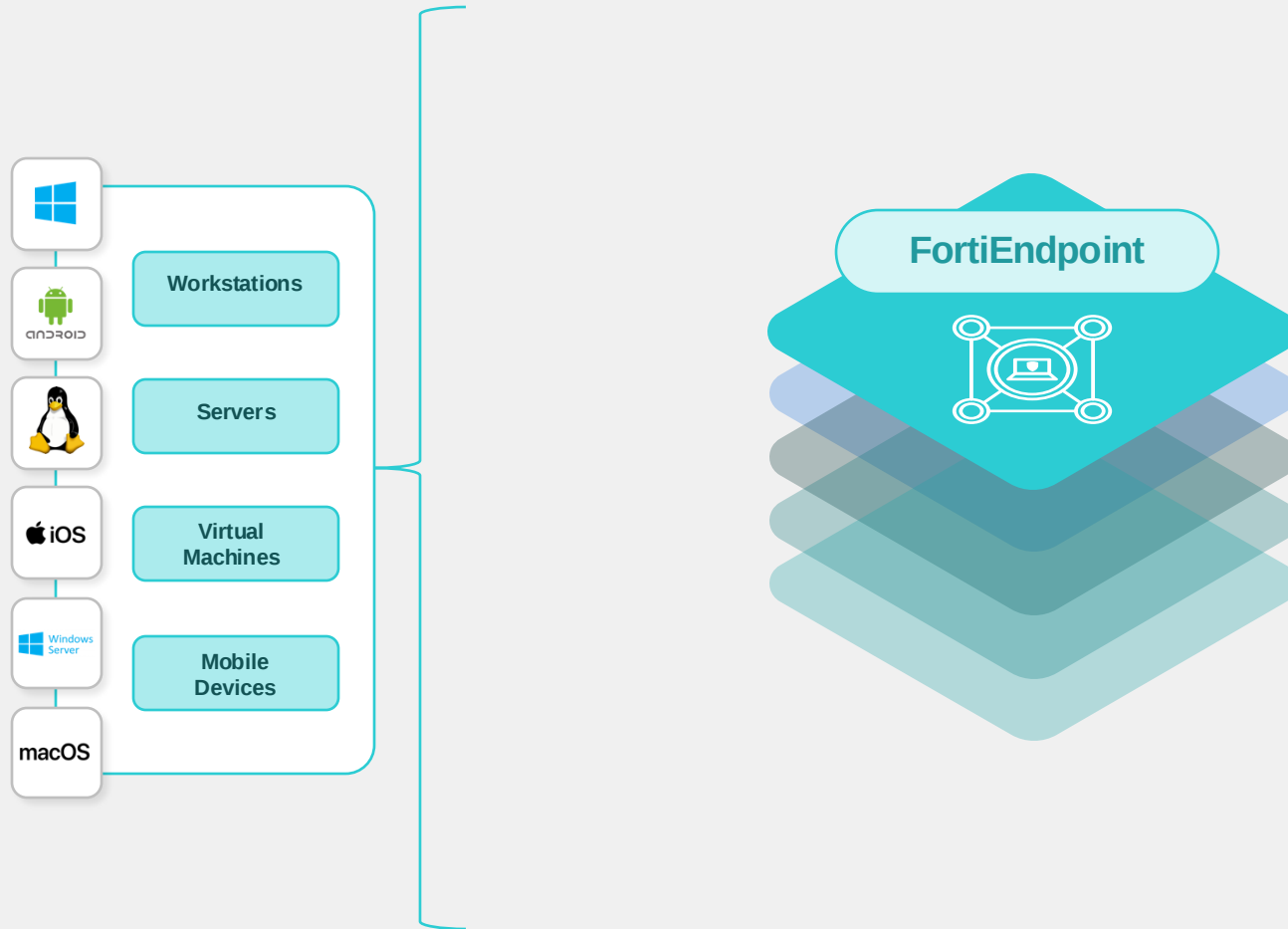
SaaS

- Subscription

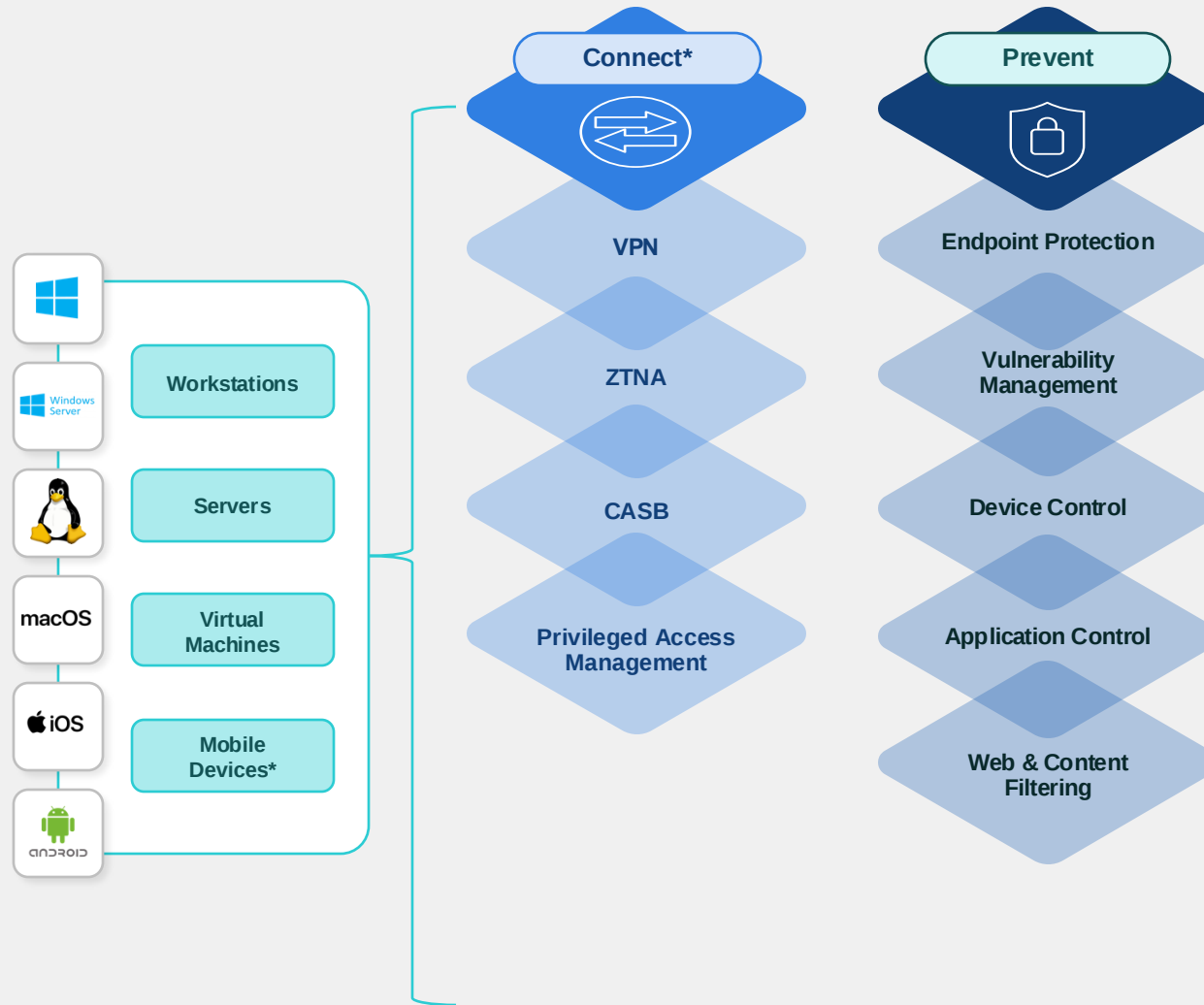


FortiEndpoint – уніфікований агент

Безпека ПК та сервісів

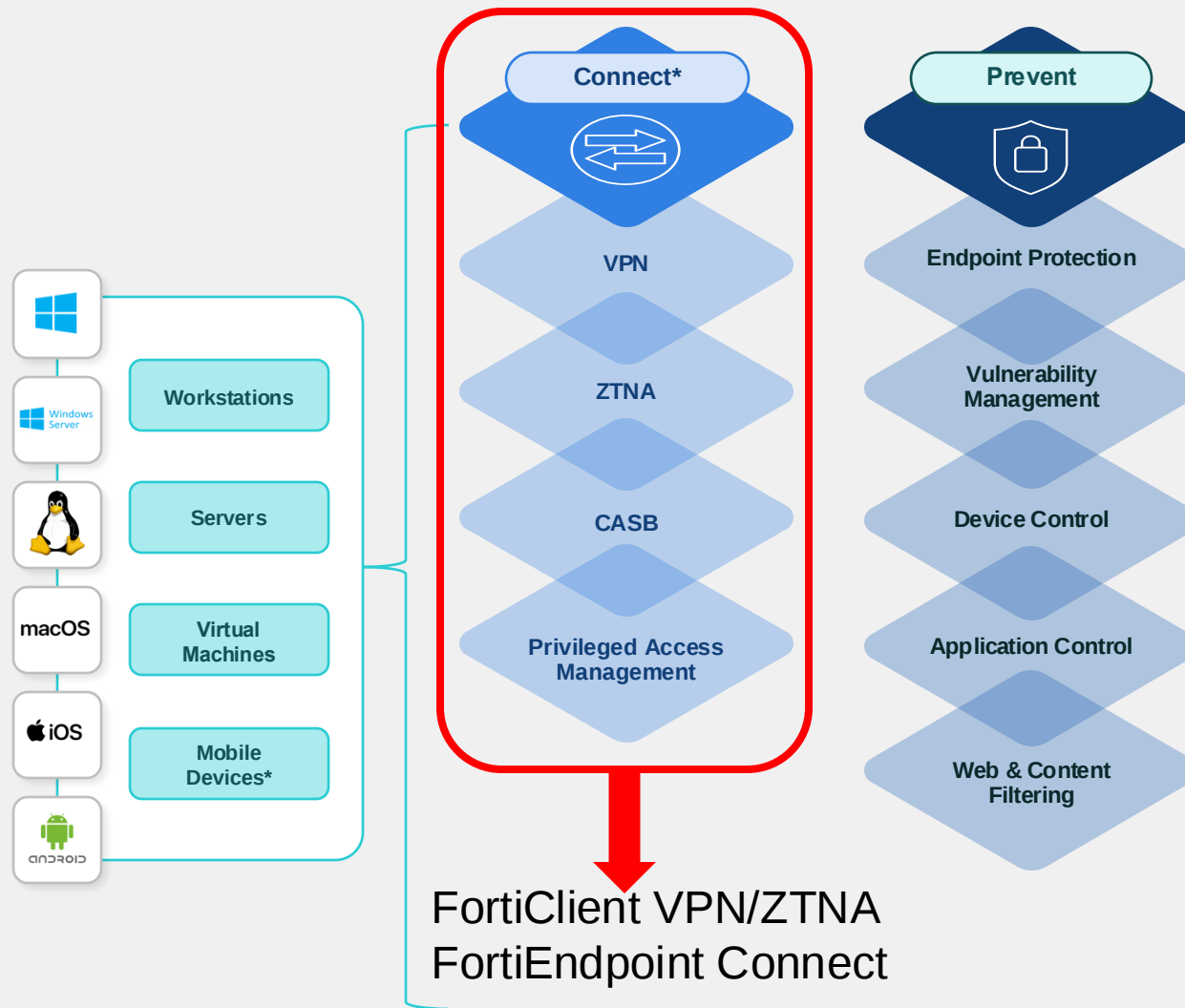


FortiEndpoint – уніфікований агент

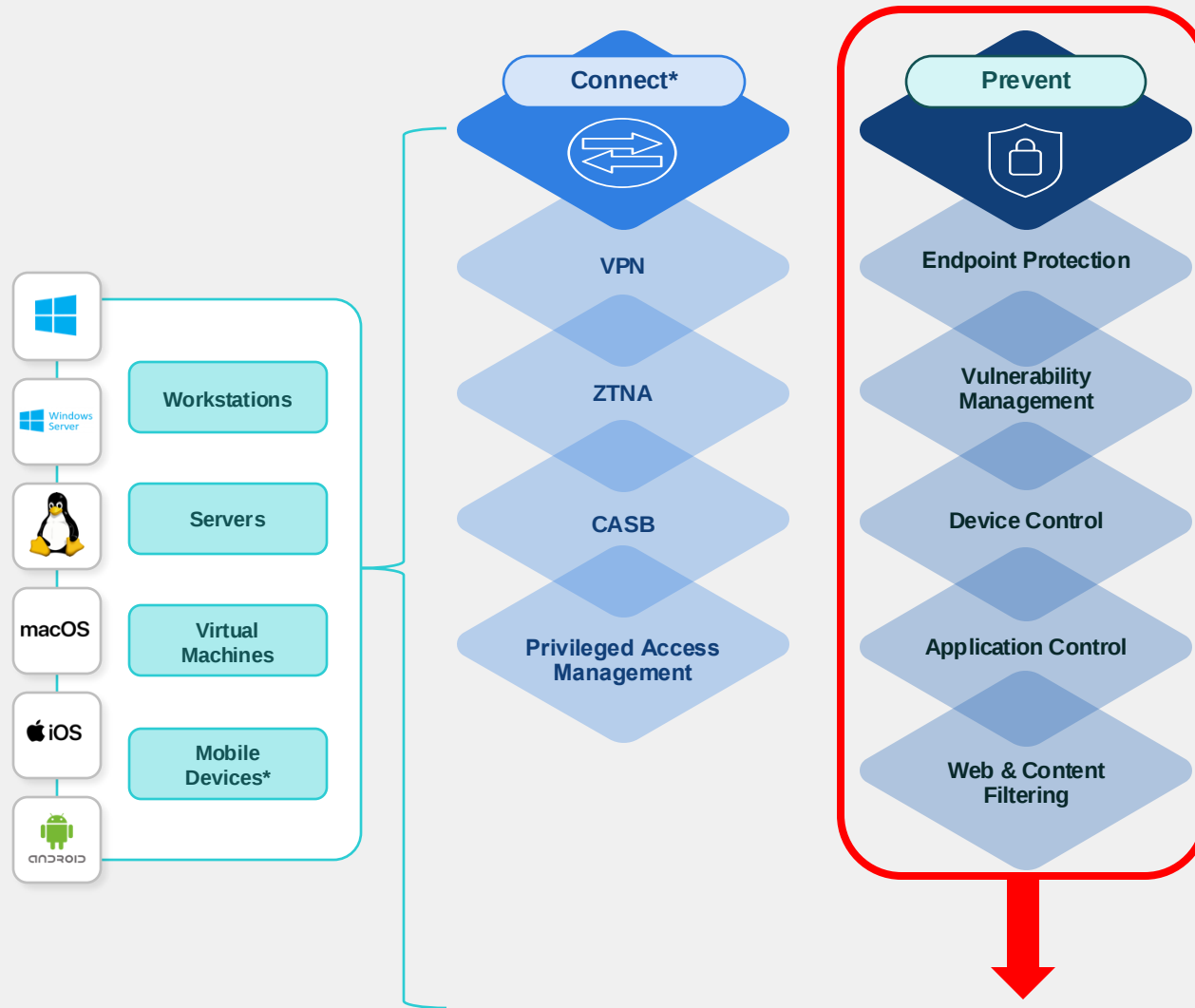


* Mobile devices not supported on EDR/XDR bundles

The Unified Agent: FortiClient Components of FortiEndpoint

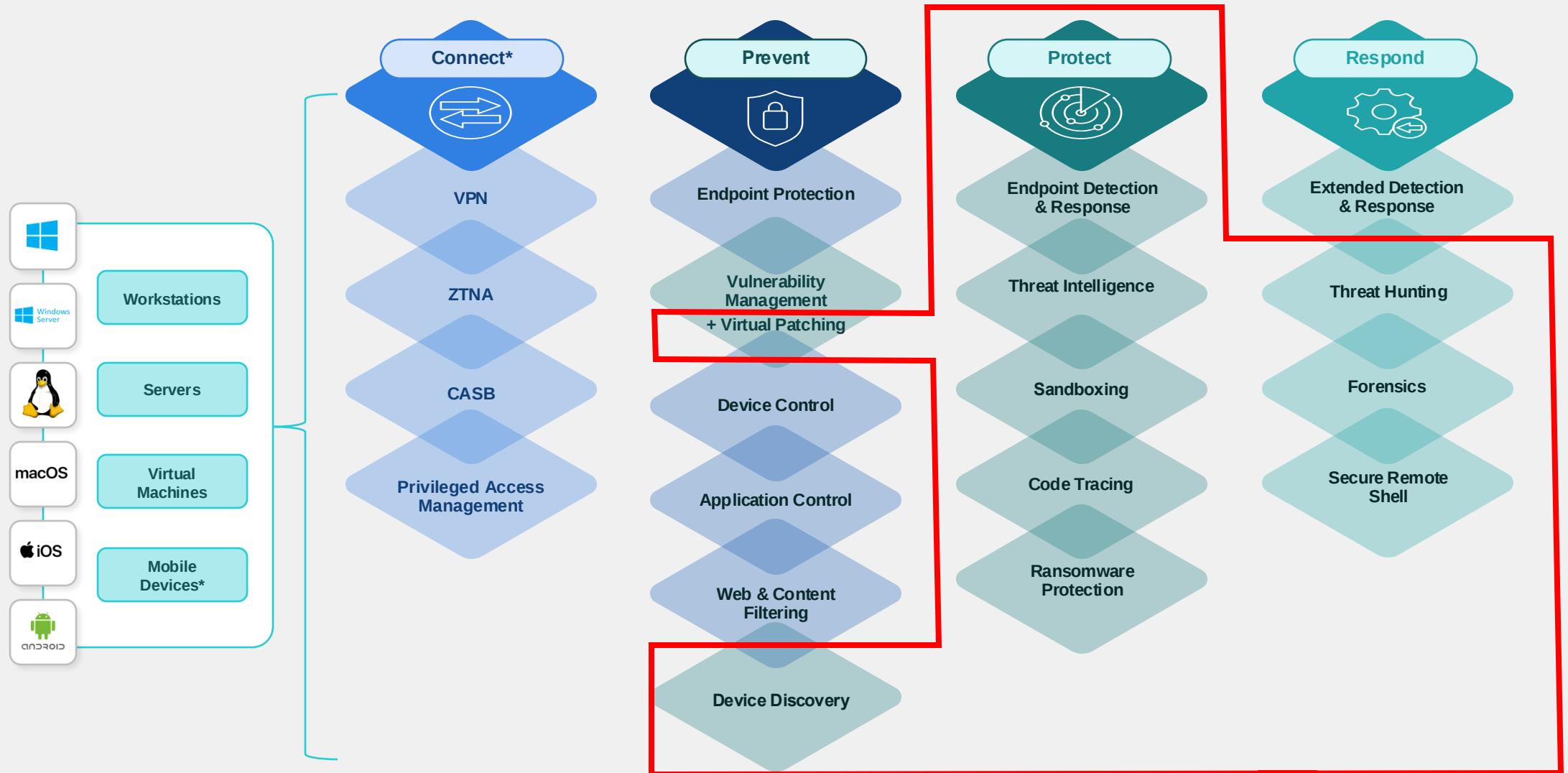


The Unified Agent: FortiClient Components of FortiEndpoint



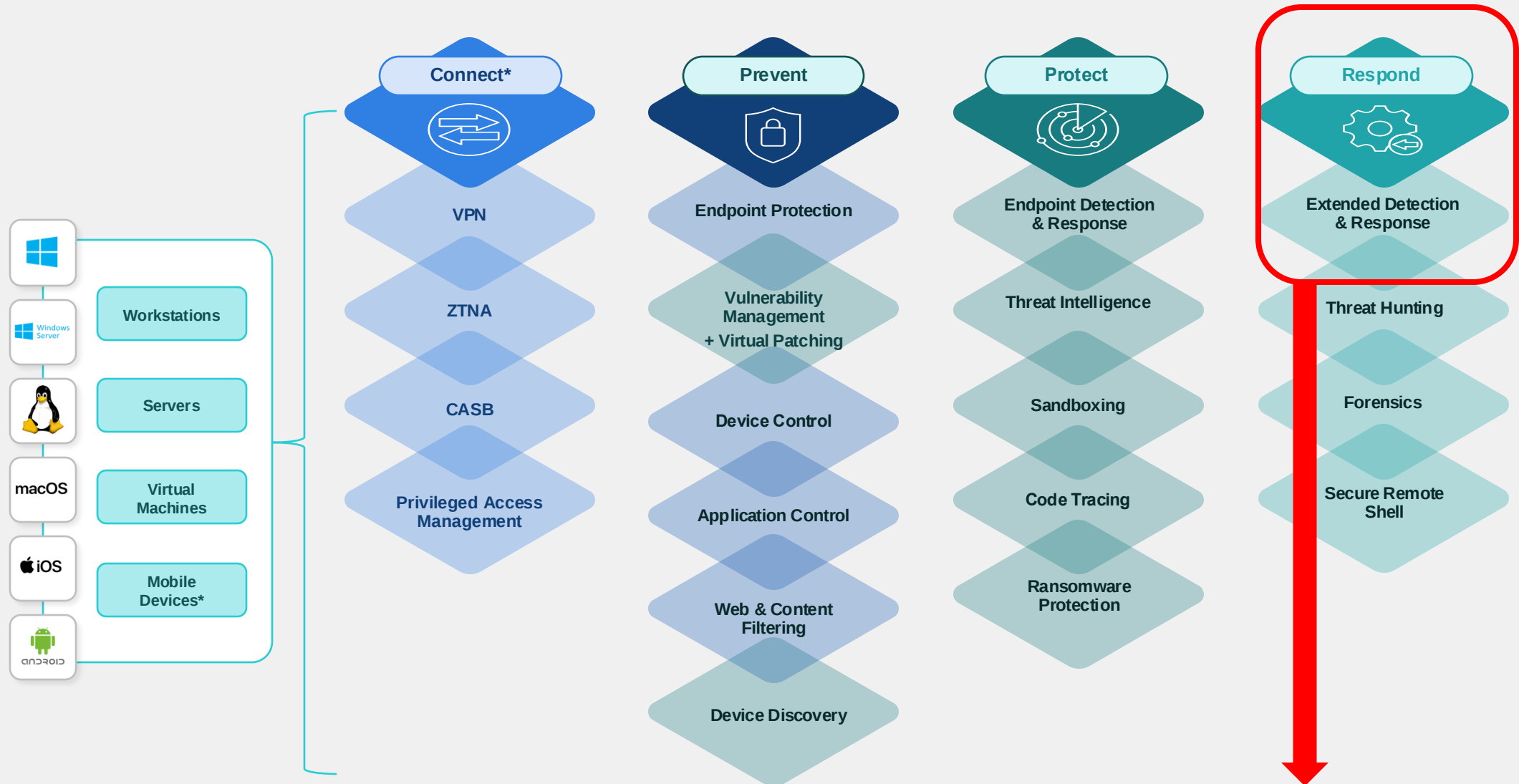
FortiClient EPP/ATP
FortiEndpoint Prevent

FortiEDR Finds Unmanaged IT and IoT Devices



FortiEDR Discover, Protect, and Respond
FortiEndpoint EDR Essentials

FortiEDR Finds Unmanaged IT and IoT Devices



FortiEDR Discover, Protect, & Respond and XDR
FortiEndpoint XDR



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.



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.



Встановлення

W11-azure-PC1

deploy741edr

172.19.200.230

Deployment 741-edr-latest

Policy Default

EMS

SYS 4

EDR 3

Summary

Vulnerability Events

EDR Events

System Events

No Email

deploy741edr

Device

W11-azure-PC1

OS

Microsoft Windows 11 , 64-bit (build 22...

IP

172.19.200.230

MAC

00-15-5d-51-36-1d

Public IP

208.91.115.30

Status

Online

Location

On-Fabric

Owner

Organization

Connection

Managed by EMS

Configuration

Policy

Default

Installer

741-edr-latest

FortiClient Version

7.4.1.5209

FortiClient Serial Number

FCT8

FortiClient ID

DECH

ZTNA Serial Number

E25E

Classification Tags

Low

Status

Managed

Features

Antivirus installed

Anti-Ransomware installed

Cloud Based Malware Outbreak Detection installed

Sandbox installed

Sandbox Cloud installed

Web Filter installed

Video Filter installed

Endpoint Detection & Response enabled

Engine Version

5.2.3.0085

EDR Enabled

Endpoint Detection & Response delivers innovative endpoint security with real-time visibility, analysis, protection, and remediation.

Activity Log: [View](#)

ZERO TRUST TELEMETRY

REMOTE ACCESS

DETECTION & RESPONSE

Back

Next

Add FortiClient Installer

3 Advanced

Endpoint Detection & Response (EDR)

Provides threat protection in real time.

Application Firewall

Inspect intrusions attempting to exploit known vulnerabilities

Single Sign-On Mobility Agent

Provides FortiAuthenticator for transparent authentication

Zero Trust Network Access

Enables FortiClient to receive a device certificate for tunneling traffic to Proxy Gateway and FortiOS.

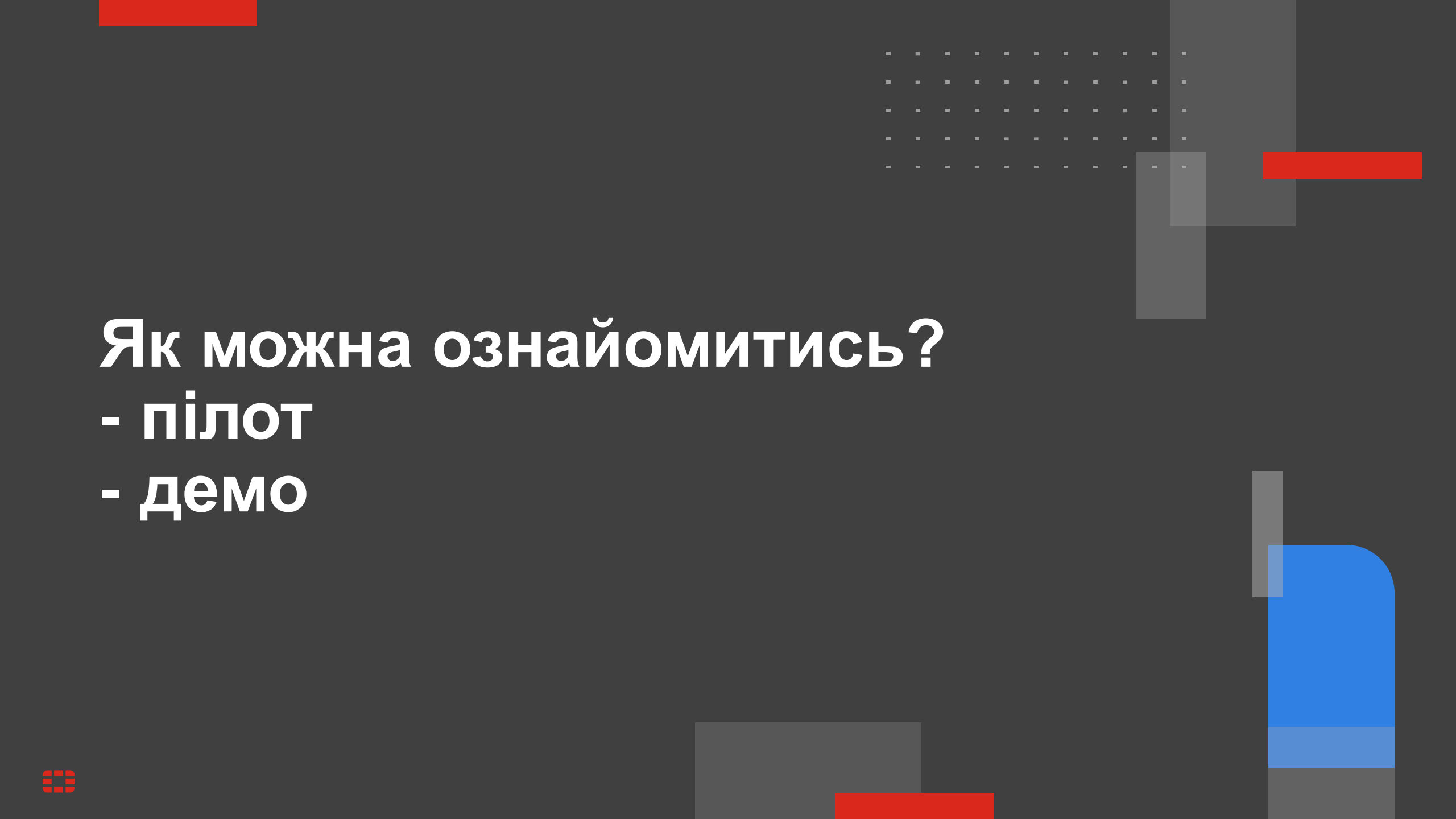
Privileged Access Agent

Privileged Access Agent

Windows features

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

© Fortinet Inc. All Rights Reserved. 56



Як можна ознайомитись?

- пілот
- демо





Євгеній Таран, Systems Engineer
ytaran@fortinet.com