Зустрічайте нове покоління FortiOS версії 7.6

Євгеній Таран, Systems Engineer

ytaran@fortinet.com

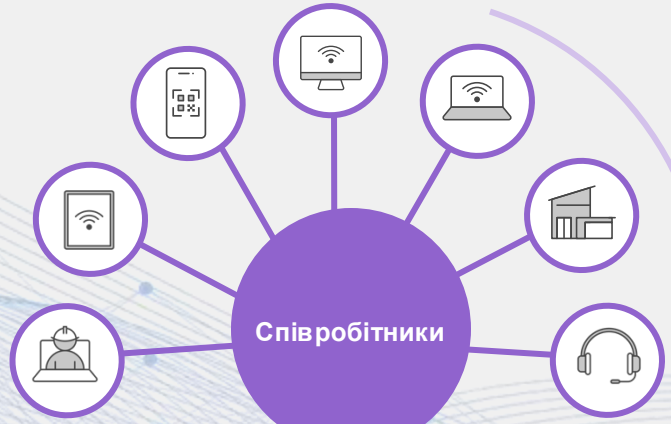
Таран Євгеній

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

P.S. Це моя друга кібервійна…

Fortinet
та поточні світові тенденції

Децентралізація та нульова довіра



84%

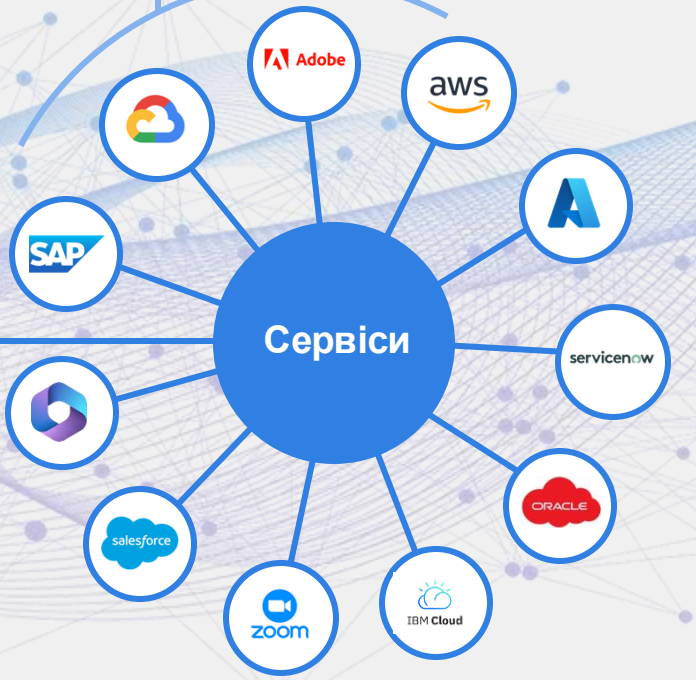
компаній гібридні

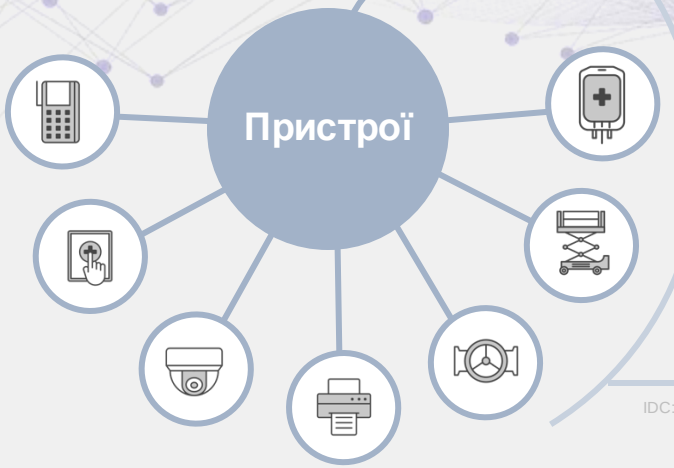
Forbes: Remote Work Statistics and Trends

125+

Різних сервісів використовуються компанією

2022 Gartner: Market Guide for SaaS Management Platforms





42 Млрд

IoT пристрої

IDC: World-Wide IDC Forecast

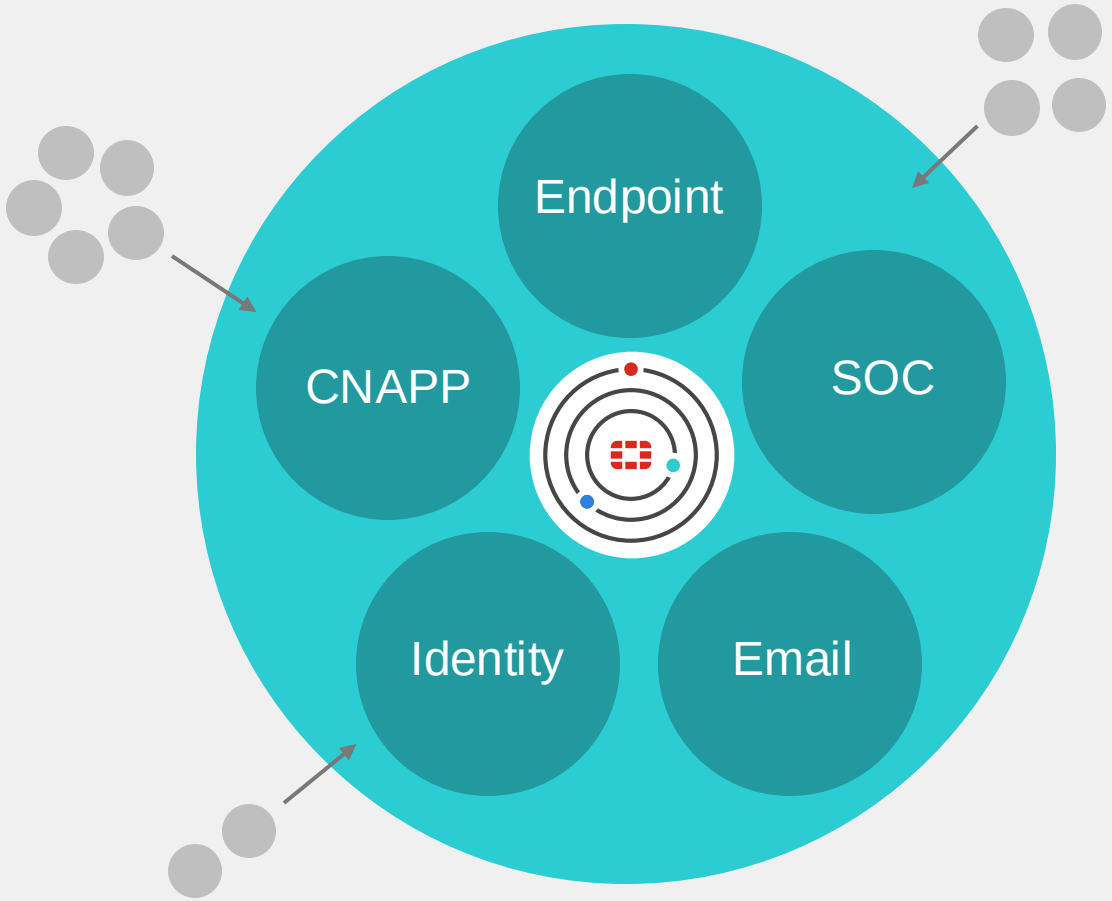
90%

Матимуть інциденти безпеки в філіях до 2026

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

Побудова IT інфраструктури

Рішення з вбудованою безпекою обженуть «традиційні» до 2026

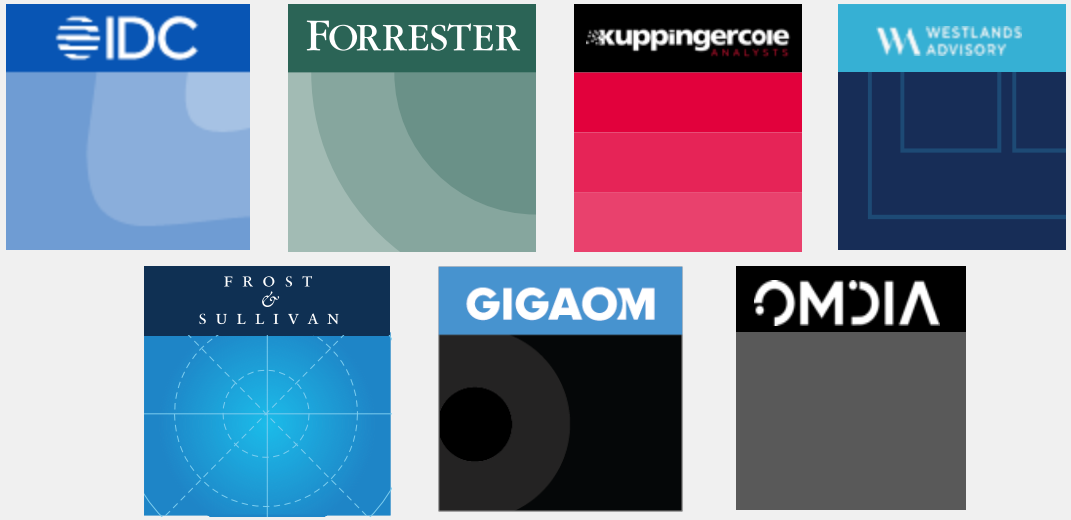


Комплекс кібербезпеки

100+

Індустрія підтверджує топові позиції Fortinet в питаннях мереж та безпеки

Fortinet є однією з найбільш перевірених компаній у світі з кібербезпеки. Fortinet постійно займає лідируючу позицію в більш ніж 100+ дослідницьких звітах від великих галузевих аналітичних фірм, таких як Gartner, IDC і Forrester, **і визнаний у 8 магічних квадрантах Gartner**.



Gartner

Leader in Magic Quadrant for SD-WAN

Gartner

Leader in Magic Quadrant for Network Firewalls

Gartner

Leader in Magic Quadrant for Enterprise Wired and Wireless LAN

Gartner

Challenger in Magic Quadrant for Single-Vendor SASE

Gartner

Challenger in Magic Quadrant for Security Service Edge

Gartner

Challenger in Magic Quadrant for Security Information and Event Management

Gartner

Niche in Magic Quadrant for Endpoint Protection Platforms

Gartner

Honorable Mention in Magic Quadrant for Access Management

Magic Quadrant for Endpoint Protection Platforms - Published 31 December 2023 - G00789052
Magic Quadrant for Security Information and Event Management - Published 10 October 2022 - ID G00755317
Magic Quadrant for SD-WAN - Published 27 September 2023 – ID G00778908
Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure – Published 06 March 2024 – G00785075
Magic Quadrant for Network Firewalls - Published 19 December 2022 - ID G00761497
Magic Quadrant for Security Service Edge - Published 10 April 2023 - ID G00766751
Magic Quadrant for Access Management - Published 16 November 2023 G 00781727
Magic Quadrant for Single-Vendor SASE - Published 16 August 2023 - ID G00785023

Єдина компанія з однією ОС

ЛІДЕР

Network Firewall

Gartner® Magic Quadrant™ for Network Firewalls – *Published 19 December 2022 – Rajpreet Kaur, Adam Hils, Thomas Lintemuth*

ЛІДЕР

SD-WAN

Gartner® Magic Quadrant™ for SD-WAN – *Published 27 September 2023 – Jonathan Forest, Naresh Singh, Andrew Lerner, Karen Brown*

ЛІДЕР

Wired & WLAN

Gartner® Magic Quadrant™ for Enterprise Wired and Wireless LAN Infrastructure – *Published 06 March 2024 – Tim Zimmerman, Christian Canales, Nauman Raja, Mike Leibovitz*

Сильний представник

Single-Vendor SASE

Gartner, Magic Quadrant™ for Single-Vendor SASE, Andrew Lerner, Jonathan Forest, Neil MacDonald, Charlie Winckless, 3 July 2024.

Сильний представник

Security Service Edge (SSE)

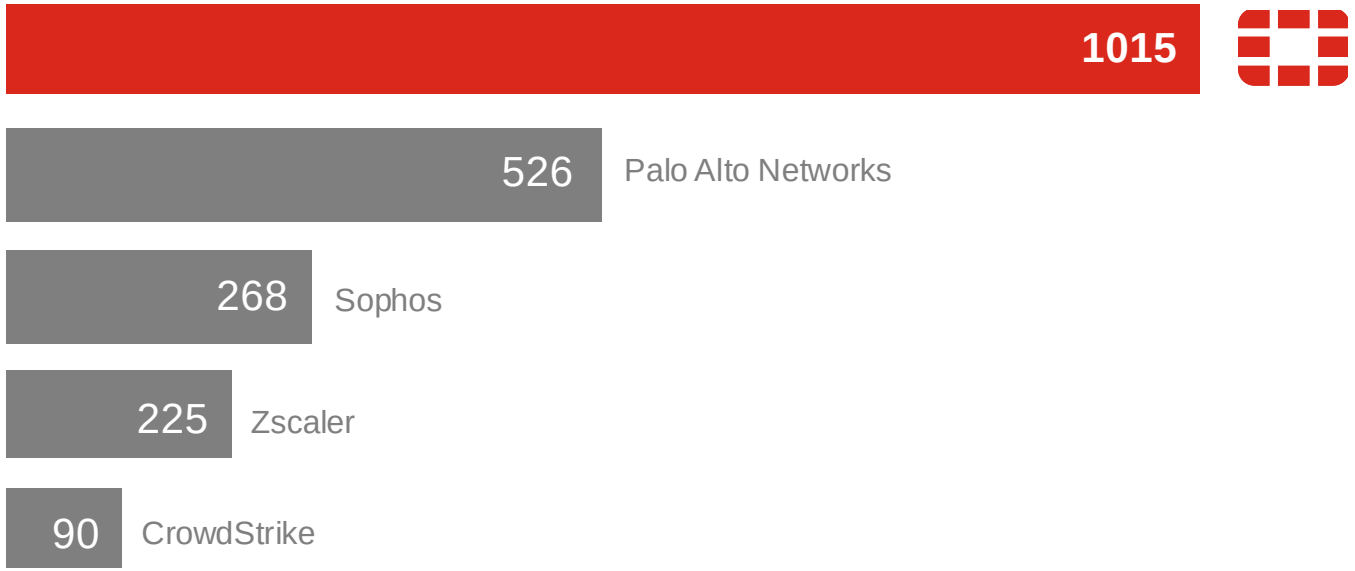
Gartner® Magic Quadrant™ for Security Service Edge – *Published 15 April 2024 – Charlie Winckless, Thomas Lintemuth, Dale Koeppen*

FortiOS

#1 новатор кібербезпеки

в 2 рази більше патентів ніж мають аналогічні компанії з кібербезпеки

Патенти США



Джерело: U.S. Patent Office, as of June 30, 2024

1354

Глобально

1,015 США

340 Інтернаціональних

454 В процесі

Включно з патентами **Lacework** та **Next DLP**

Fortinet портфоліо

Безпечна мережа

Мережева безпека

- **FortiGate** Firewall
- **FortiGate VM** Virtual Firewall
- **FortiCNF** Cloud-native Firewall
- **FGaaS** Firewall-aaS
- **FortiGate** Rugged NGFW

Корпоративні мережі

- **FortiSwitch** Switching
- **FortiAIOps** AI For Networking
- **FortiAP** Access Point
- **FortiNAC** NAC
- **FortiSwitch** Rugged Switch
- **FortiExtender** LTE/5G
- **FortiAP** Rugged AP
- **FortiExtender** Rugged Extender

FortiManager
Centralized Management

Уніфікований SASE

Безпека доступу

- **FortiSASE** SSE
- **FortiGate** SD-WAN
- **FortiClient** ZTNA
- **FortiProxy** SWG
- **FortiMonitor** DEM
- **FortiCASB** CASB

Хмарна безпека

- **FortiGate VM** Virtual Firewall
- **FortiWeb** (WAAP)
- **FortiGate CNF** Cloud-native Firewall
- **FortiADC** Application Delivery

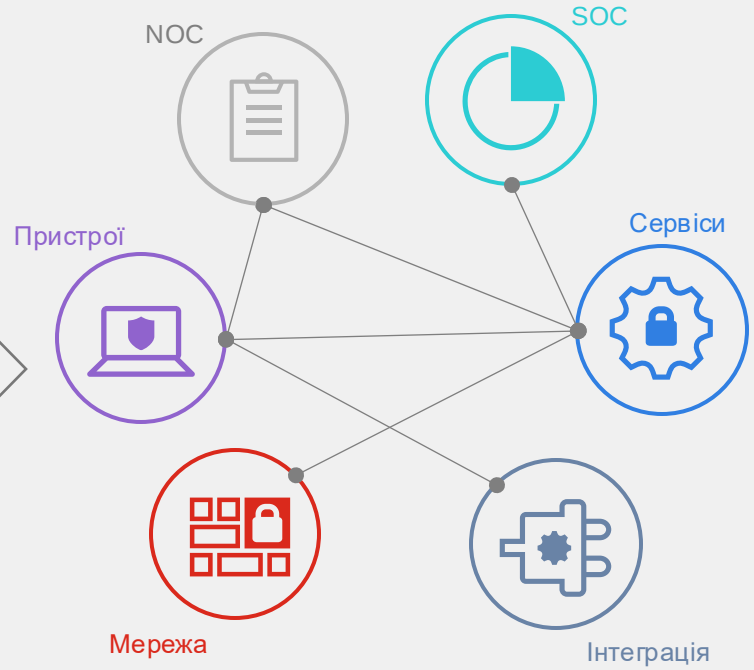
SOC

- **Lacework FortiCNAPP**
- **FortiNDR** NDR
- **FortiAnalyzer** Analytics
- **FortiEDR/XDR** EDR/XDR
- **FortiSIEM** SIEM
- **SOCaaS**
- **FortiDeceptor** Deception
- **FortiSOAR** SOAR
- **MDR Service**
- **FortiRecon** DRPS
- **FortiSandbox** Sandbox
- **IR Service**
- **FortiAuthenticator** Cloud
- **FortiPAM** PAM
- **FortiMail** SEG
- **FortiToken** MFA
- **FortiDLP** DLP
- **FortiTrust** Identity

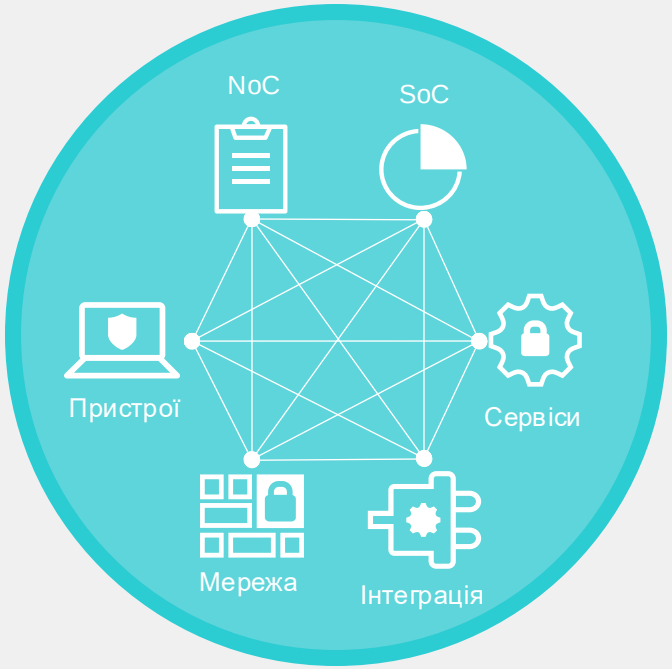
Еволюція

30+ виробників

10 виробників



2-3 платформи



Розвиток Вашого IT

Комплексне рішення Fortinet

Основи FortiGate

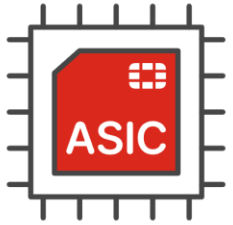
Firewall

Основа

FortiOS

30 мережевих та безпекових функцій

ASIC



Лідер індустрії в розрізі ціна/швидкодія та енергоефективність

Найпотужніша ОС мережевої безпеки

FortiOS органічно підтримує 30+ мережевих та безпекових функцій

Єдині пропрієтарні ASIC

Чим більше функцій включено в ОС тим більше потужності потрібно для їх реалізації. Як GPU важливі для графіку та TPU штучного інтелекту в світі безпеки ASIC прискорюють роботу за рахунок виконання функцій знімаючи їх з CPU.

Security Processor 5
SP5

ASIC «все в одному» що включає CPU, обробку контенту та мережевого трафіку

Network Processor 7
NP7

NP7 архітектура дозволяє досягти малих затримок та досягати роботи безпеки в режимі реального часу

FortiASIC покращує FortiOS та її швидкодію

FortiSP5 підтримує в 2 рази більше функцій ніж чіп попереднього покоління

Швидкодія та функції

2 функції

Anti-Malware
Firewall

SP2

4 функції

IPS
IPSEC

Anti-Malware
Firewall

SP3

7 функцій

SD-WAN
SSL

NGFW

IPS
IPSEC
Anti-Malware
Firewall

SP4

14 функцій

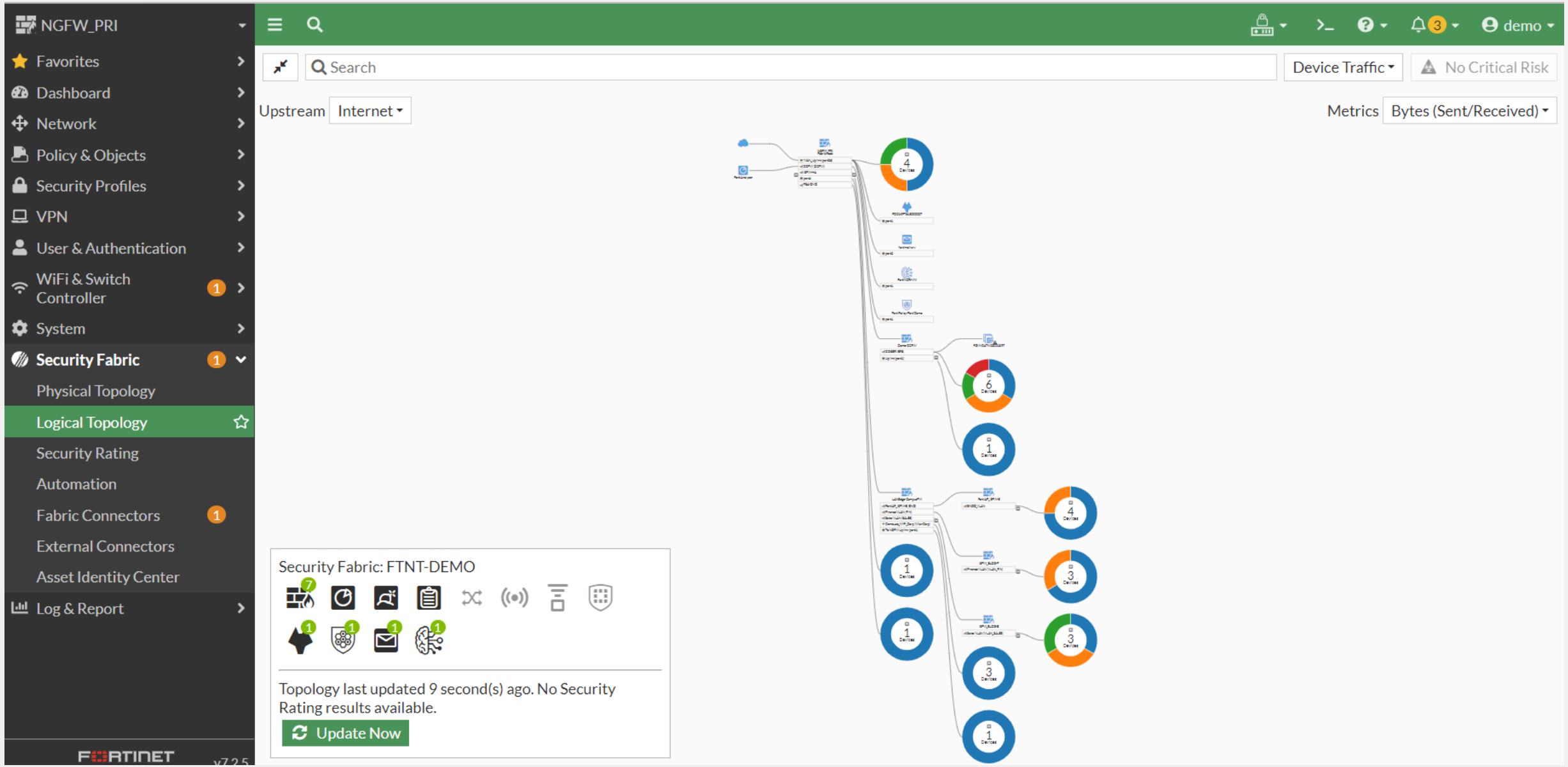
SD-Branch
Zero Trust
OT
5G
Edge Compute
VXLAN

Secure Boot

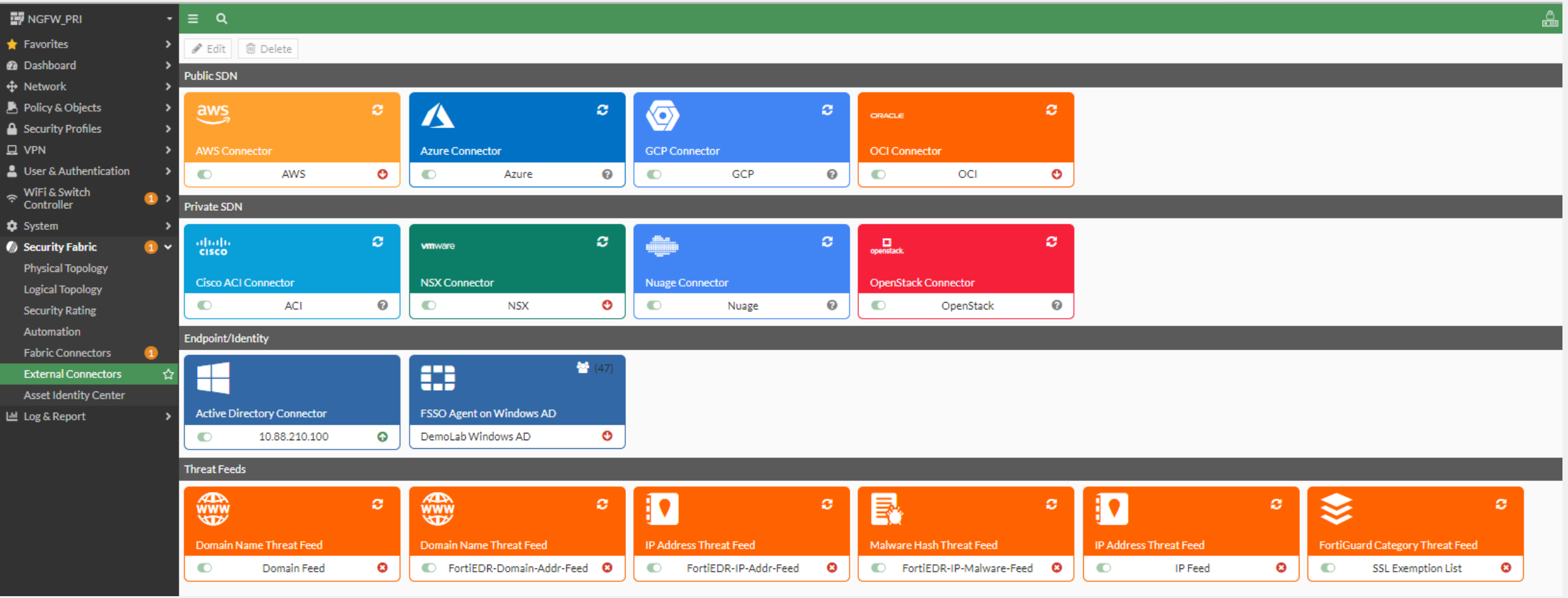
SD-WAN
SSL
NGFW
IPS
IPSEC
Anti-Malware
Firewall

SP5

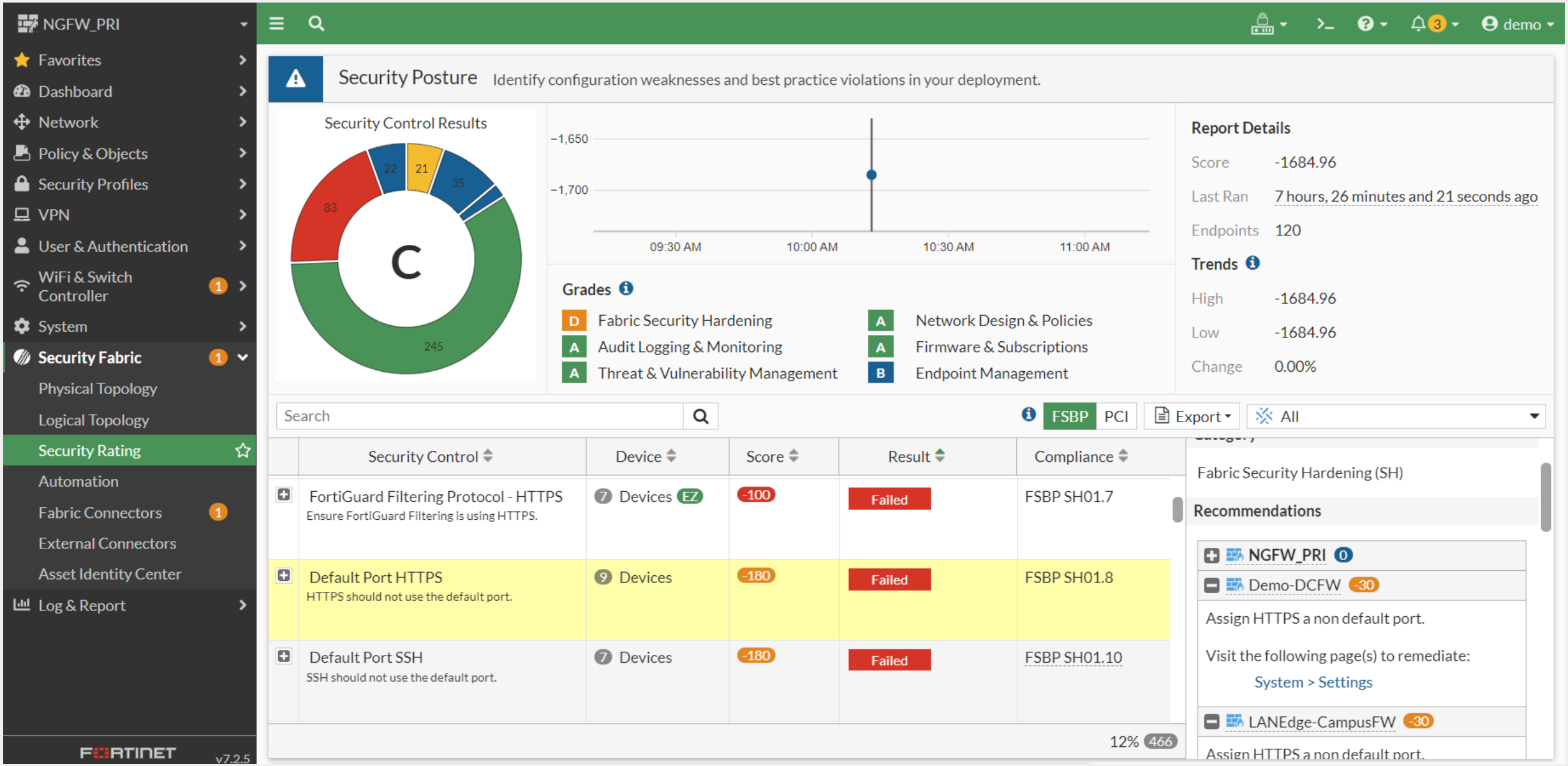
FortiGate Security Fabric



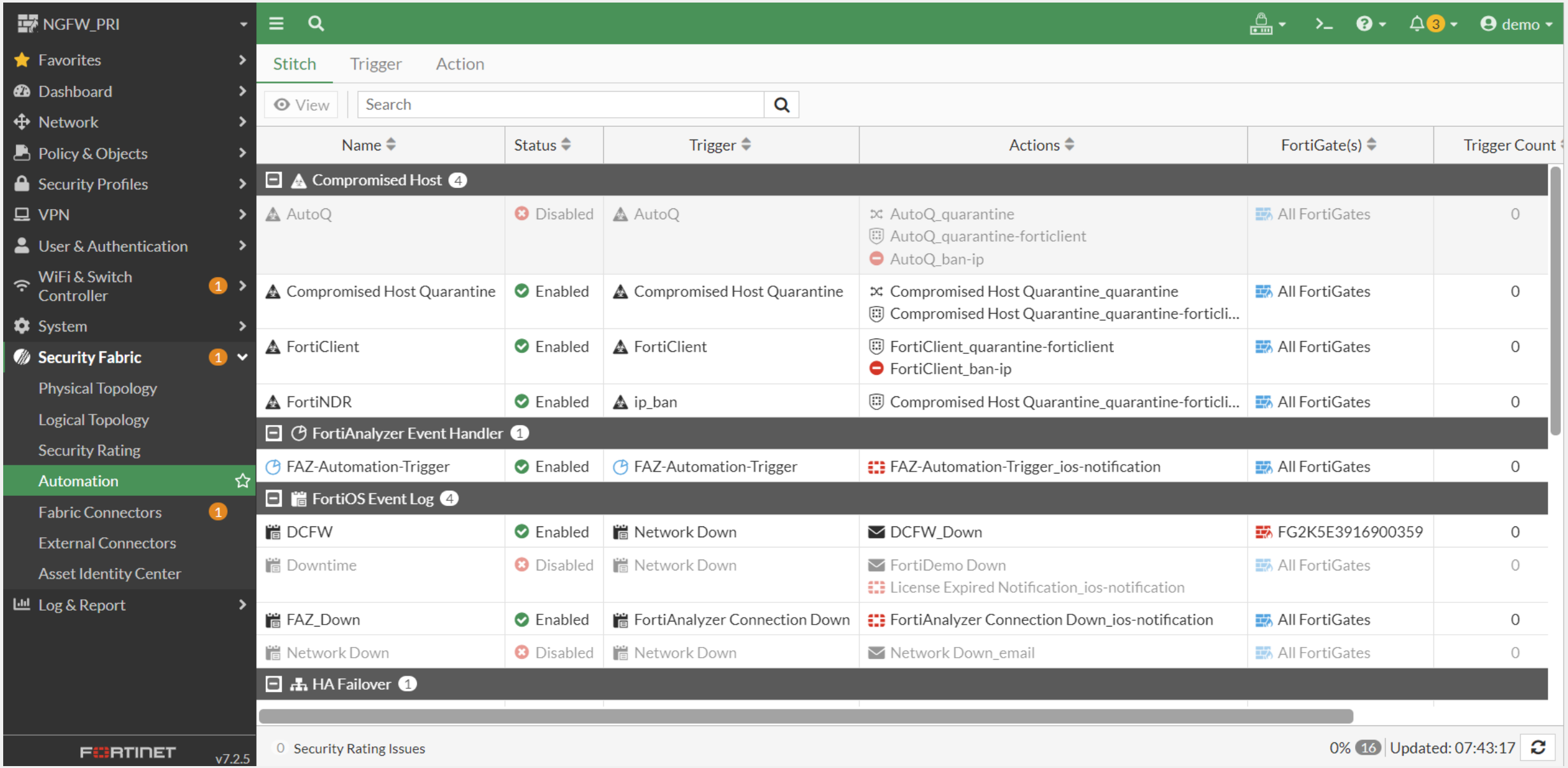
FortiGate Security Fabric



FortiGate Security Fabric



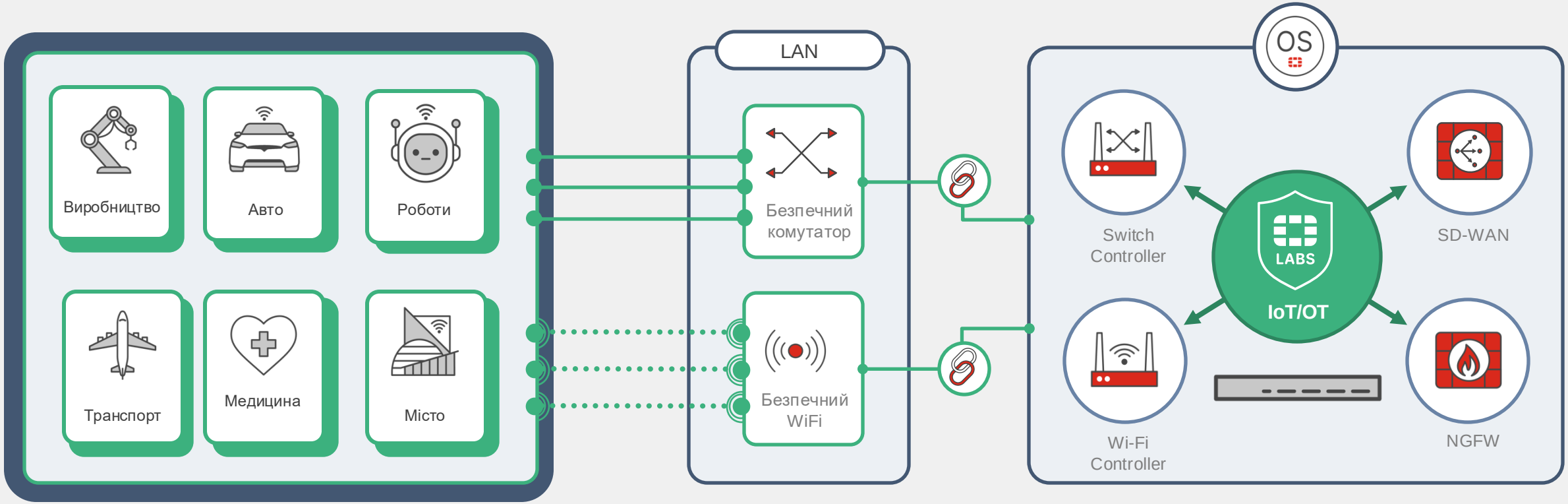
FortiGate Security Fabric



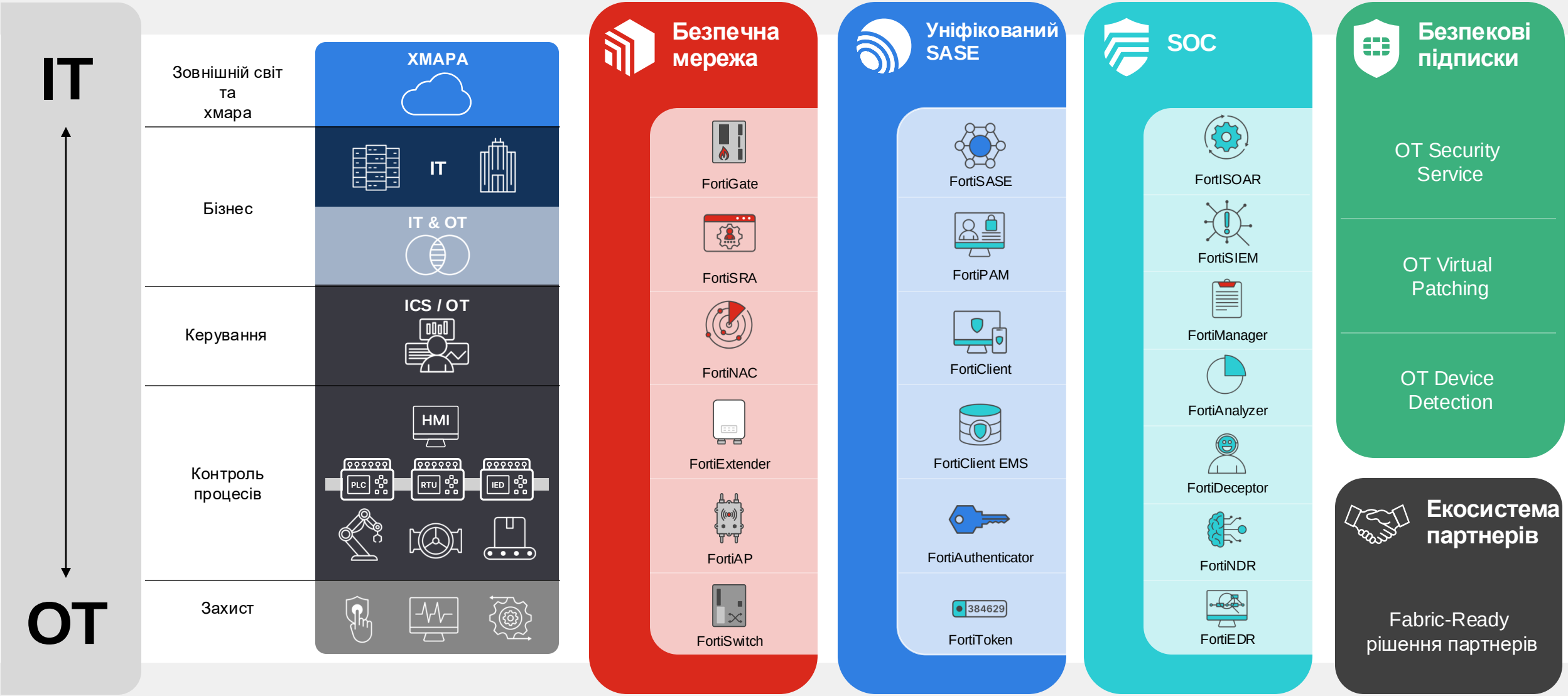
OT/IoT безпека

Безпека без агентів

IoT/OT пристрої мають великі обмеження щодо запуску будь якого ПЗ безпеки

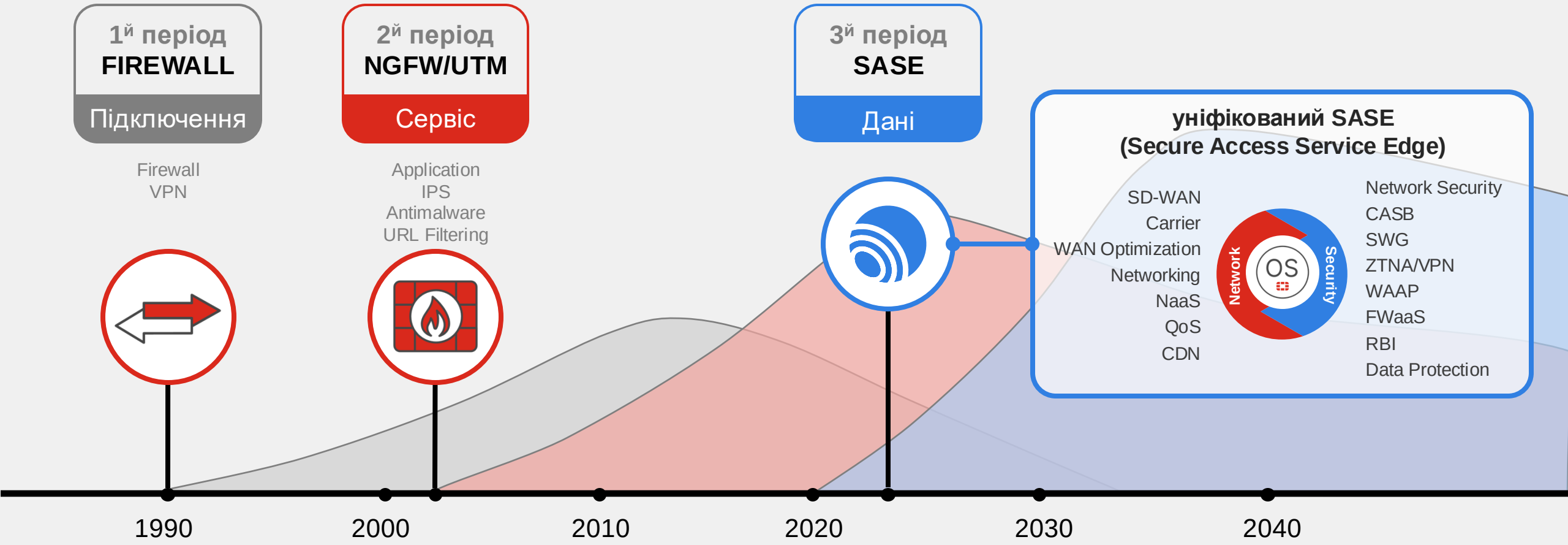


Платформа безпеки Fortinet OT

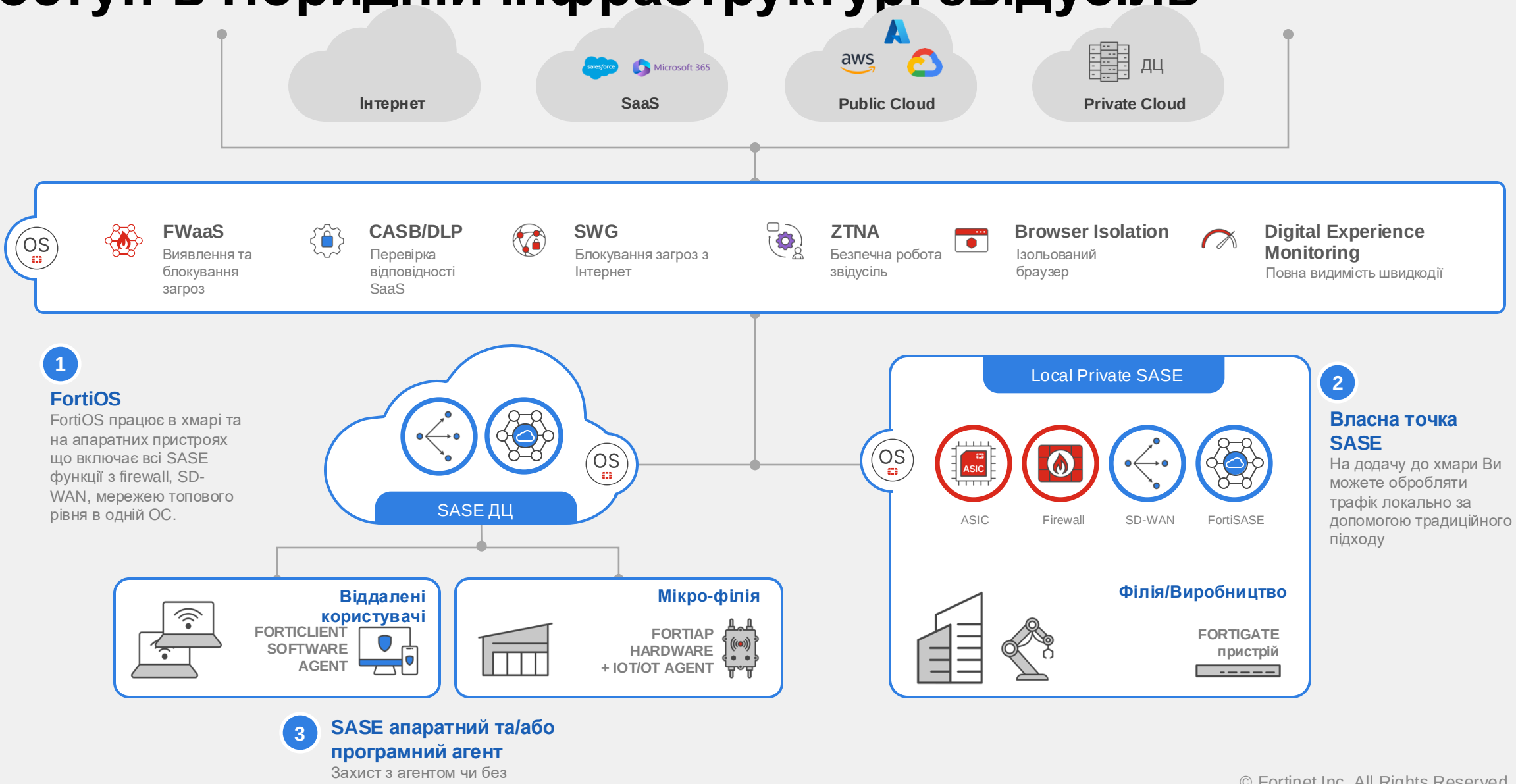


Уніфікований SASE

Еволюція мережевої безпеки



Уніфікований SASE дозволяє реалізувати безпечний доступ в гібридній інфраструктурі звідусіль



Версії FortiOS

Трохи про поточне ПЗ

Recommended software

Technical Tip: Recommended Release for FortiOS

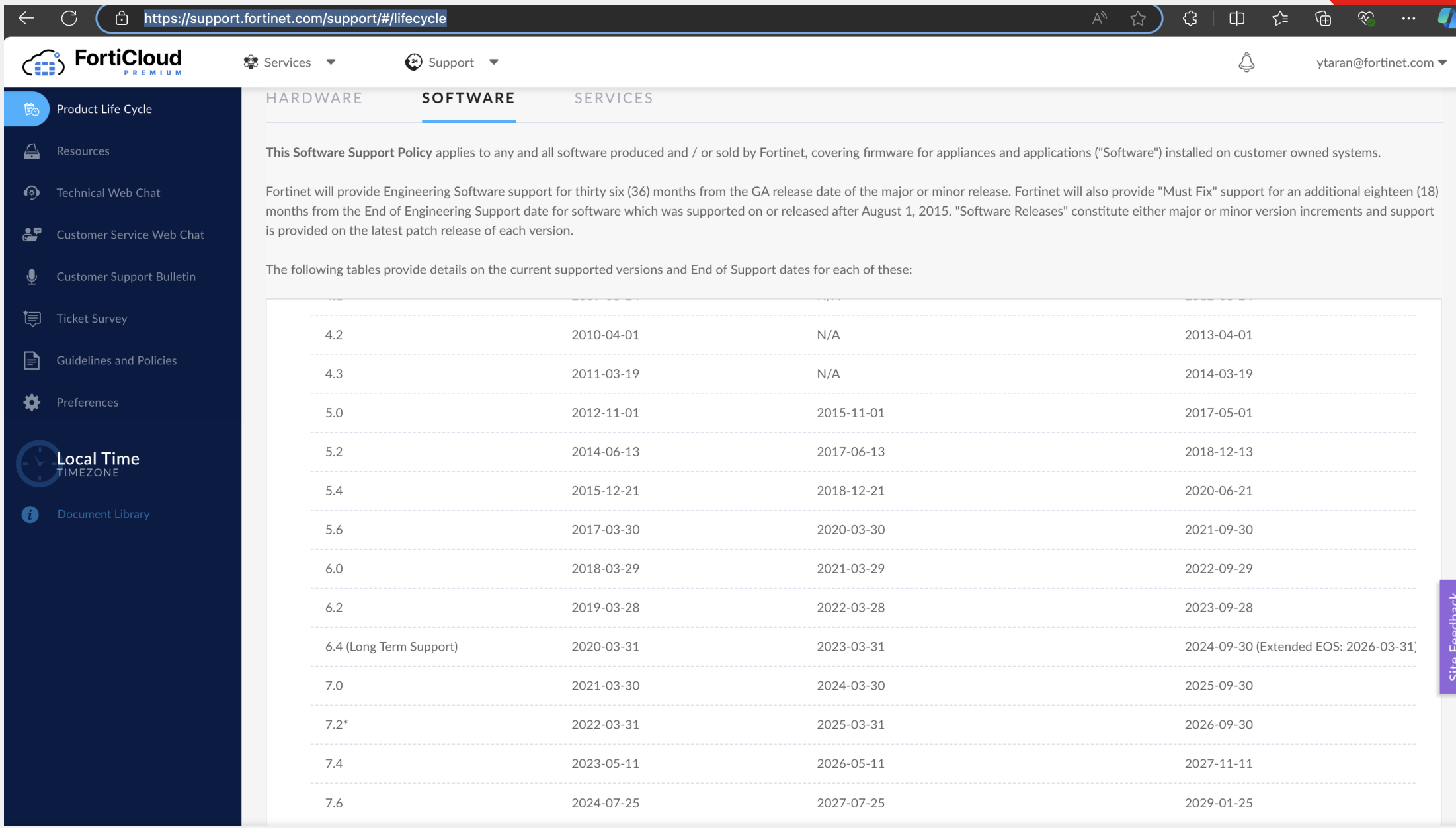
Description	This article exists to help customers determine the most appropriate software release for FortiOS. The recommendations stated below are the latest as of April 2024 and are reviewed and updated every quarter. The information in this document is not meant to be exhaustive and is intended to serve as general guidance to customers, especially in cases of mass deployments/upgrades. When working with Fortinet SEs, Professional Services, or TAC: it is important to refer to their specific guidance. Additional FAQ added for related questions about this article. Subscribe/RSS feed by clicking on the three-dotted menu button to keep up to date on the latest changes to this article.
Scope	This document is a general recommendation of FortiOS Software recommendations for general customer deployments for general stability and is updated on a **quarterly** basis. For customers who may be leveraging the latest features, the latest FortiOS versions may be more applicable.
Solution	

Product Family	Product Details	Recommended Release	End of Engineering Support Passed (Y/N)
	FortiGateRugged-35D	6.2.16	Y
	FortiGate-30E	6.2.16	Y
	FortiWiFi-30E	6.2.16	Y
	FortiGate-40F	7.2.7	N
	FortiWiFi-40F	7.2.7	N
	FortiGate-40F-3G4G	7.2.7	N
	FortiWiFi-40F-3G4G	7.2.7	N
	FortiGate-50E	6.2.16	Y
	FortiWiFi-50E	6.2.16	Y
	FortiGate-51E	6.2.16	Y
	FortiWiFi-51E	6.2.16	Y
	FortiGate-52E	6.2.16	Y
	FortiGate-60E	7.2.7	N
	FortiWifi-60E	7.2.7	N
	FortiGate-60F	7.2.7	N
	FortiWiFi-60F	7.2.7	N
Low End	FortiGate-61F	7.2.7	N

[Netflow sampling | FortiGate / FortiOS 7.6.0 | Fortinet Document Library]

EoS

На прикладі FortiGate



[Fortinet Document Library | Upgrade Path Tool]

EoS детальніше

На прикладі FortiGate

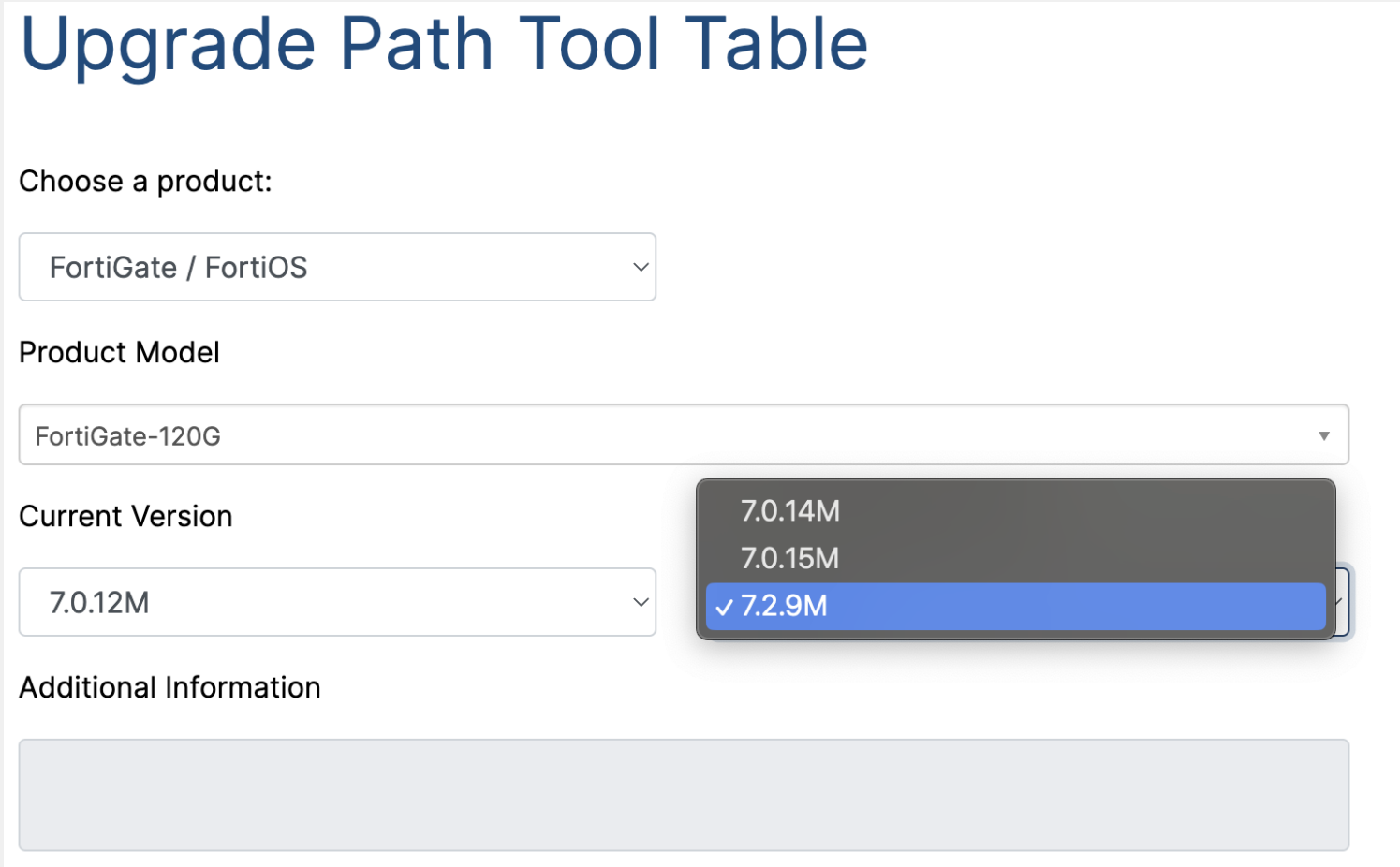
FortiOS

SOFTWARE VERSION	RELEASE DATE (GA)	END OF ENGINEERING SUPPORT DATE (EOES)	END OF SUPPORT DATE (EOS)
6.4 (Long Term Support)	2020-03-31	2023-03-31	2024-09-30 (Extended EOS: 2026-03-31)
7.0	2021-03-30	2024-03-30	2025-09-30
7.2*	2022-03-31	2025-03-31	2026-09-30
7.4	2023-05-11	2026-05-11	2027-11-11
7.6	2024-07-25	2027-07-25	2029-01-25

Fortinet Document Library | Upgrade Path Tool

Версії ПЗ

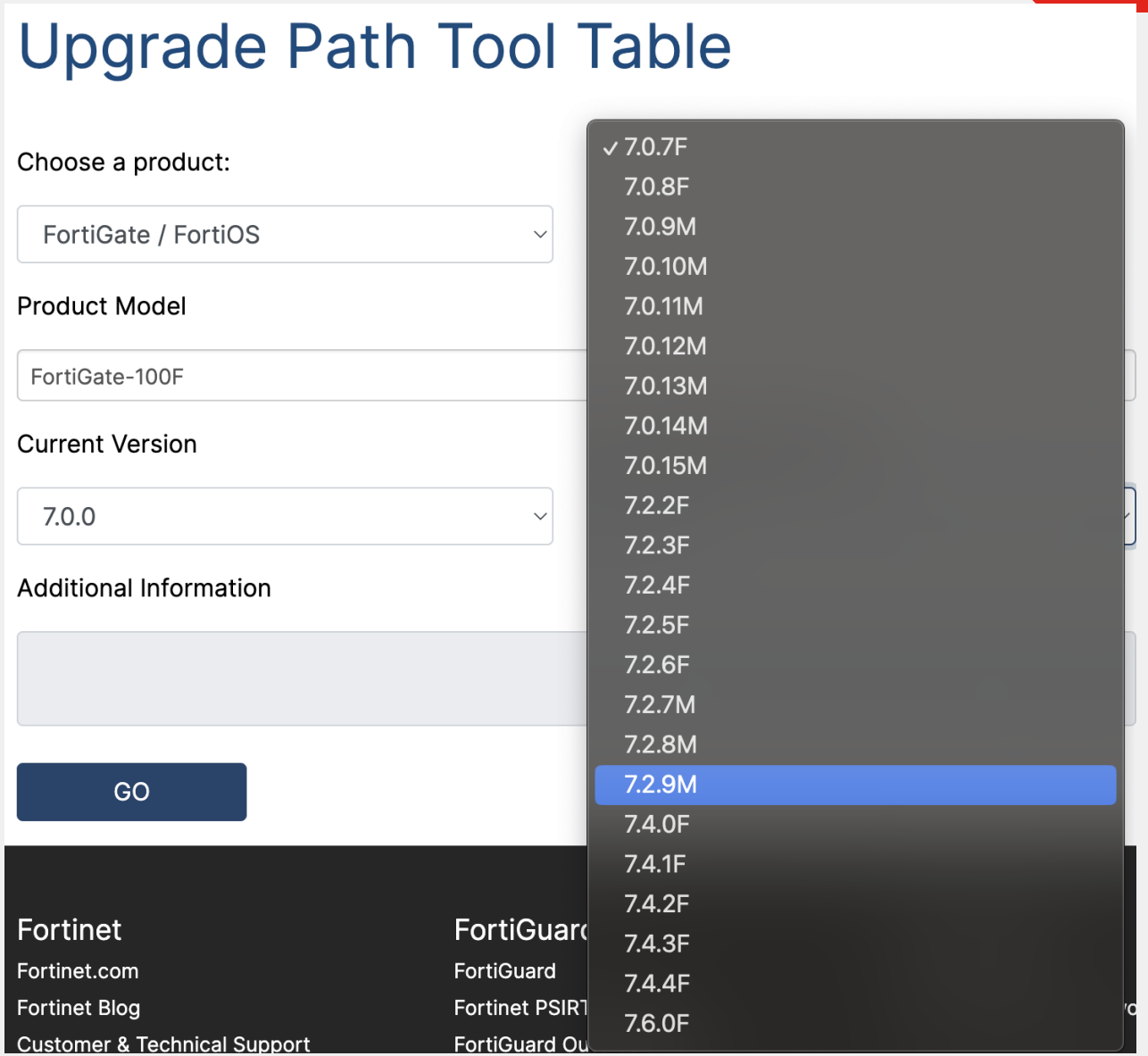
На прикладі FortiGate 120G



[Fortinet Document Library | Upgrade Path Tool]

Версії ПЗ

На прикладі FortiGate 100F



[Fortinet Document Library | Upgrade Path Tool]

Нове в FortiOS

Нарешті новини

NetFlow sampling

Статистика трафіку

Netflow sampling

FortiOS supports NetFlow sampling, allowing it to maintain a count of the number of packets or bytes that have been sampled for an interface. If the packet count for a session surpasses the configured threshold for transmitted or received traffic on a NetFlow-enabled interface, a NetFlow report is exported. This helps reduce the load on the collector.

```
config system interface
    edit <name>
        set netflow-sampler {tx | rx | both}
        set netflow-sample-rate <integer>
        set netflow-sampler-id <integer>
    next
end
```

`netflow-sampler {tx | rx | both}`	Enable/disable NetFlow on this interface and set the data that NetFlow collects.
`netflow-sample-rate <integer>`	NetFlow sample rate. Sample one packet every configured number of packets (1 - 65535, default = 1, which means standard NetFlow where all packets are sampled).
`netflow-sampler-id <integer>`	NetFlow sampler ID.

[Netflow sampling | FortiGate / FortiOS 7.6.0 | Fortinet Document Library]

Automatic LTE connection establishment

Бездротовий зв'язок

7.6.0

Automatic LTE connection establishment

This information is also available in the FortiOS 7.6 Administration Guide:

- Automatic LTE connection establishment

Establishing an LTE connection is now automated. When you insert a SIM card into FortiGate, FortiOS can obtain the Mobile Country Code (MCC) and Mobile Network Code (MNC) from the service provider's radio tower. FortiOS then uses the codes to look up the appropriate APN for the SIM card in a predefined table and automatically creates a wireless profile. Manual configuration is no longer needed, which simplifies the process of establishing an LTE connection.

Automatic LTE connection establishment | FortiGate / FortiOS 7.6.0 | Fortinet Document Library

ADVPN 2.0 enhancements

Покращення роботи з маршрутами

ADVPN 2.0 enhancements

This information is also available in the FortiOS 7.6 Administration Guide:

- ADVPN 2.0 edge discovery and path management

ADVPN 2.0 operation has been enhanced for SD-WAN. ADVPN 2.0 edge discovery and path management was introduced in FortiOS 7.4.2. See ADVPN 2.0 edge discovery and path management.

The following enhancements have been added:

- The local spoke directly sends a shortcut-query to a remote spoke to trigger a shortcut after ADVPN 2.0 path management makes a path decision.
- ADVPN 2.0 path management can trigger multiple shortcuts for load balancing SD-WAN rules. Traffic can be load balanced over these multiple shortcuts to use as much of the available WAN bandwidth as possible without wasting idle links if they are healthy. The algorithm to calculate multiple shortcuts for the load balancing service will consider transport group and in-SLA status for both local and remote parent overlays.
- Spokes can automatically deactivate all shortcuts connecting to the same spoke when user traffic is not observed for a specified time interval. This is achieved by enabling a shared idle timeout setting in the IPsec VPN Phase 1 interface settings for associated overlays.

ADVPN 2.0 enhancements | FortiGate / FortiOS 7.6.0 | Fortinet Document Library

HTTP transaction logging

Пошук несправностей веб трафіку або розслідування інцидентів

HTTP transaction details are logged in a new type of traffic log when HTTP traffic is routed through a proxy. This ensures comprehensive logging of HTTP interactions for improved monitoring and analysis.

After an HTTP transaction is proxied through the FortiGate, traffic logs of the http-transaction subtype are generated in addition to the forward subtype log. HTTP transaction logs are based on each transaction, such as an HTTP request and response pair. When there are multiple HTTP transactions completed over the TCP connection there will be multiple http-transaction logs and only one forward traffic log.

HTTP transaction logging can be enabled in explicit-web proxy, transparent-web proxy, access-proxy, and proxy-mode firewall policies.

```
config firewall proxy-policy
    edit 1
        set proxy {explicit-web | transparent-web | access-proxy}
        logtraffic {utm | all}
        set log-http-transaction {enable | disable}
    next
end
config firewall policy
    edit 1
        set inspection-mode proxy
        logtraffic {utm | all}
        set log-http-transaction {enable | disable}
    next
end
```

[HTTP transaction logging | FortiGate / FortiOS 7.6.0 | Fortinet Document Library]

HTTP transaction logging

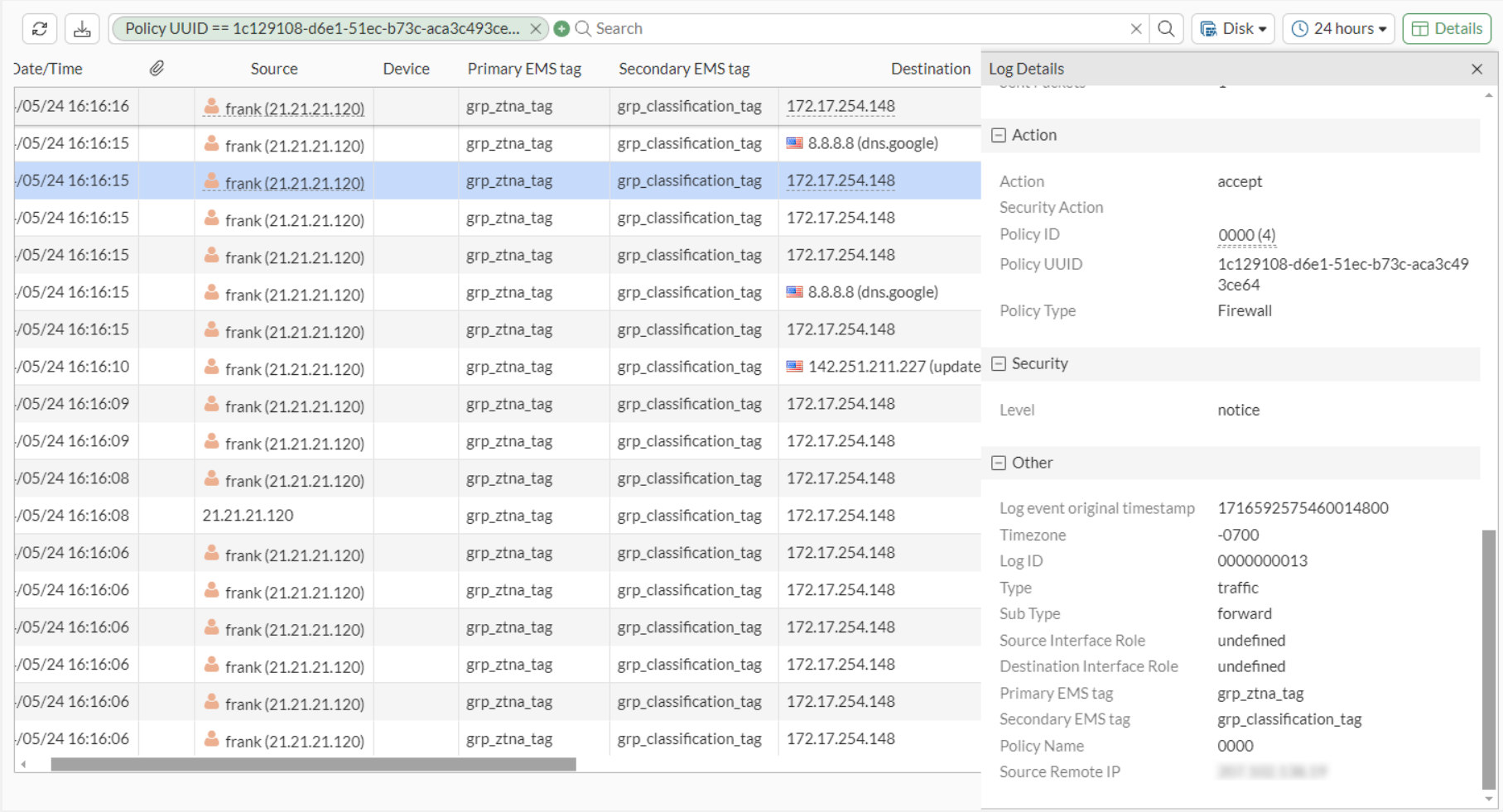
Пошук несправностей веб трафіку або розслідування інцидентів

```
1: date=2024-05-21 time=20:06:17 eventtime=1716347177537010993 tz="-0700" logid="0000000010" type="traffic"
subtype="forward" level="notice" vd="vdom1" srcip=10.1.100.11 srcport=42694 srcintf="port1"
srcintfrole="undefined" dstcountry="Reserved" srccountry="Reserved" dstip=172.16.200.44 dstport=80
dstintf="port3" dstintfrole="undefined" sessionid=316483733 service="HTTP" proxyapptype="web-proxy" proto=6
action="accept" policyid=1 policytype="proxy-policy" poluuid="1e1e0b2e-14c1-51ef-7b4c-6b789be487f2"
trandisp="snat" transip=172.16.200.8 transport=12204 duration=30 wanin=760 rcvdbyte=760 wanout=211 lanin=163
sentbyte=163 lanout=36194 appcat="unscanned" utmaction="block" countav=1 utmref=65515-14

2: date=2024-05-21 time=20:06:17 eventtime=1716347177536946272 tz="-0700" logid="0006000026" type="traffic"
subtype="http-transaction" level="notice" vd="vdom1" srcip=10.1.100.11 srcport=42694 dstip=172.16.200.44
dstport=80 sessionid=316483733 transid=50331679 action="accept" policyid=1 policytype="proxy-policy"
poluuid="1e1e0b2e-14c1-51ef-7b4c-6b789be487f2" url="http://172.16.200.44/eicar.com" agent="curl/7.68.0"
duration=0 reqlength=86 resplength=392 rcvdbyte=760 sentbyte=163 scheme="http" hostname="172.16.200.44"
resptype="cached" httpmethod="GET" statuscode="403" reqtime=1716347177 resptime=0 respfinishtime=1716347177
appcat="unscanned" utmaction="block" countav=1 utmref=65515-0

3: date=2024-05-21 time=20:06:06 eventtime=1716347166400042072 tz="-0700" logid="0006000026" type="traffic"
subtype="http-transaction" level="notice" vd="vdom1" srcip=10.1.100.11 srcport=42694 dstip=172.16.200.44
dstport=80 sessionid=316483733 transid=50331678 action="accept" policyid=1 policytype="proxy-policy"
poluuid="1e1e0b2e-14c1-51ef-7b4c-6b789be487f2" url="http://172.16.200.44/" agent="curl/7.68.0" duration=0
reqlength=77 resplength=368 rcvdbyte=368 sentbyte=77 scheme="http" hostname="172.16.200.44" resptype="normal"
httpmethod="GET" statuscode="200" reqtime=1716347166 resptime=1716347166 respfinishtime=1716347166
appcat="unscanned"
```

[HTTP transaction logging | FortiGate / FortiOS 7.6.0 | Fortinet Document Library]

Include EMS tag information in traffic logs

Більше видимості результату перевірок EMS



[Include EMS tag information in traffic logs | FortiGate / FortiOS 7.6.0 | Fortinet Document Library]

Bomain fronting protection

Перевірка домену в запити і в header відповіді

FortiOS now protects against domain fronting in both explicit proxy and proxy-based firewall policies. In both cases, FortiGate checks whether the domain of the request matches the host domain in the HTTP header, and then allows, blocks, or monitors the traffic. This feature enhances security by preventing unauthorized access that could result from domain mismatches.

The `config firewall profile-protocol-options` command includes a new option:

```
config firewall profile-protocol-options
    edit protocol
        config http
            set domain-fronting {allow | block | monitor}
        next
    end
end
```

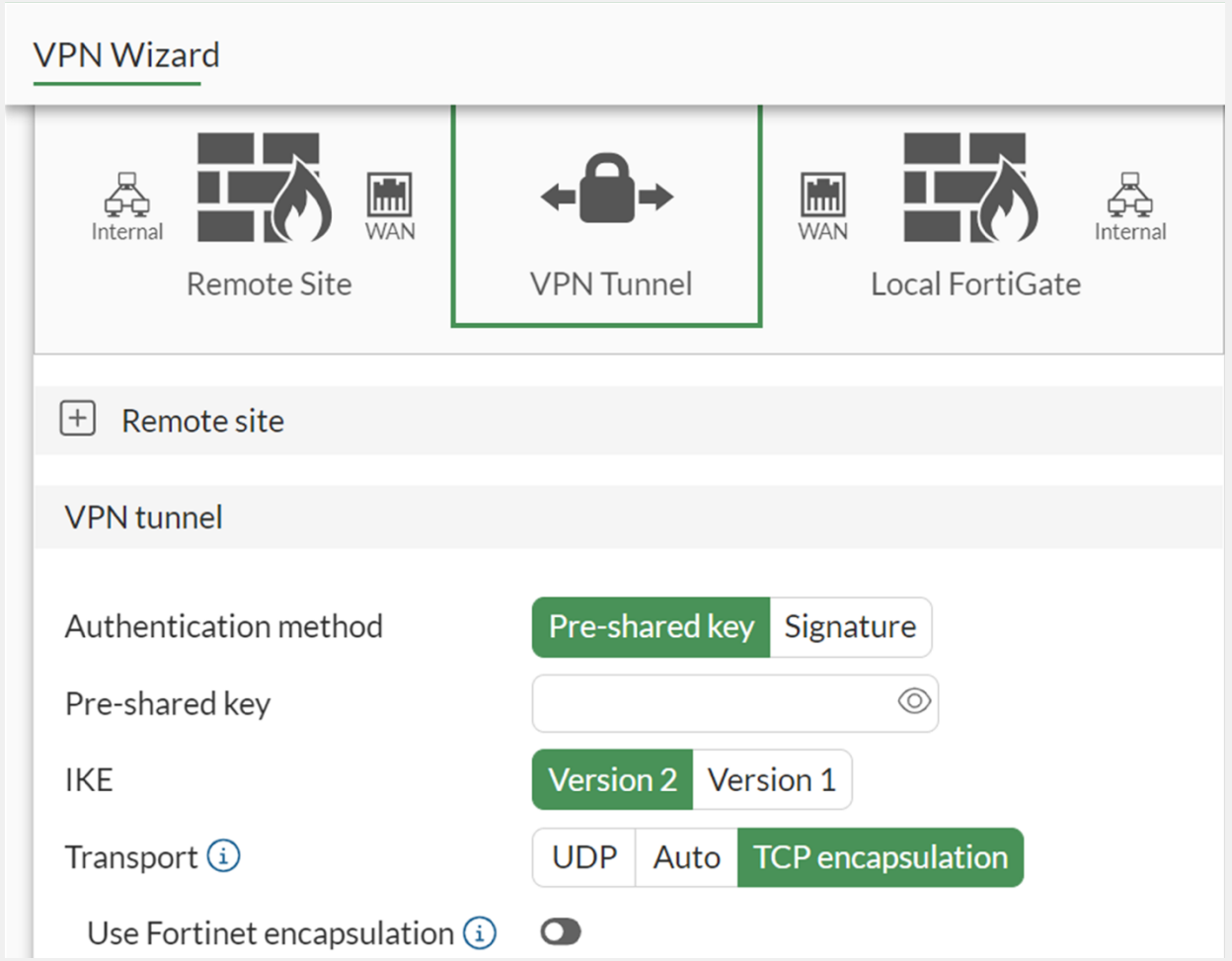
`set domain-fronting {allow | block | monitor}`	Configure HTTP domain fronting (default = block). • `allow`: allow domain fronting. • `block`: block and log domain fronting. • `monitor`: allow and log domain fronting.

Domain fronting protection supports HTTP/1.1 but not HTTP/2.

[Introducing domain fronting protection | FortiGate / FortiOS 7.6.0 | Fortinet Document Library]

Automatic selection of IPsec tunneling protocol

+1 зручність



[Automatic selection of IPsec tunneling protocol | FortiGate / FortiOS 7.6.0 | Fortinet Document Library]

Security posture tag match enforced before dial-up IPsec VPN connection

In an IPsec dial-up VPN configuration, an option is added to enforce ZTNA security posture tag matching before establishing a VPN tunnel. When a tag is defined on an IKEv2 IPsec tunnel, the client IP addresses that are resolved by that tag will be allowed to establish connection to the tunnel. When multiple tags are used, tags are checked sequentially until a match is made. If no tags match, then the client cannot establish a VPN connection.

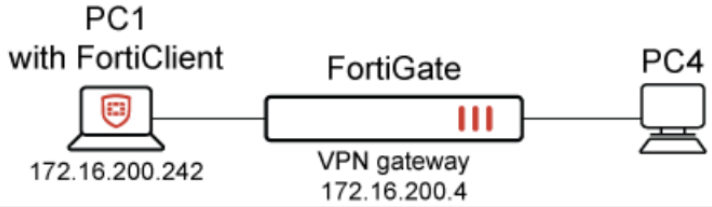
The following settings have been added:

```
config vpn ipsec phase1-interface
    edit <name>
        set ike-version 2
        set remote-gw-match {any | ipmask | iprange | geography | ztna}
        set remote-gw-ztna-tags <IPv4 ZTNA posture tags>
    next
end
```

When `set remote-gw-match ztna` is enabled, `remote-gw-ztna-tags` can be configured.

Example

A PC (172.16.200.242) makes a connection to the dial-up VPN gateway (172.16.200.4). The following example configuration and outputs show a successful connection with a matching ZTNA security posture tag (`EMS1_ZTNA_all_registered_clients`) and an unsuccessful connection when a ZTNA security posture tag cannot be matched.



[Security posture tag match enforced before dial-up IPsec VPN connection | FortiGate / FortiOS 7.6.0 | Fortinet Document Library]

Support the 802.11mc protocol in FortiAP

Більш точний роумінг

This release adds support for the 802.11mc Wi-Fi protocol, which enables supported devices and clients to measure their distance to nearby Wi-Fi access points. APs act as a Fine Timing Measurement (FTM) responder to time measurement queries sent from a client.

FortiAP radios can be configured to operate in 802.11mc responder mode, enabling connected devices and clients to use enhanced location accuracy.

The FortiAP must be running firmware version 7.6.0 or later to support this feature.

The following CLI configuration setting has been added:

```
conf wireless-controller wtp-profile
  edit <name>
    config radio-1
      set 80211mc [enable | disable]
    end
  next
end
```

[Support the 802.11mc protocol in FortiAP | FortiGate / FortiOS 7.6.0 | Fortinet Document Library]

GUI support for configuring wireless data rates and sticky client thresholds

[Add GUI support for configuring wireless data rates and sticky client thresholds | FortiGate / FortiOS 7.6.0 | Fortinet Document Library]

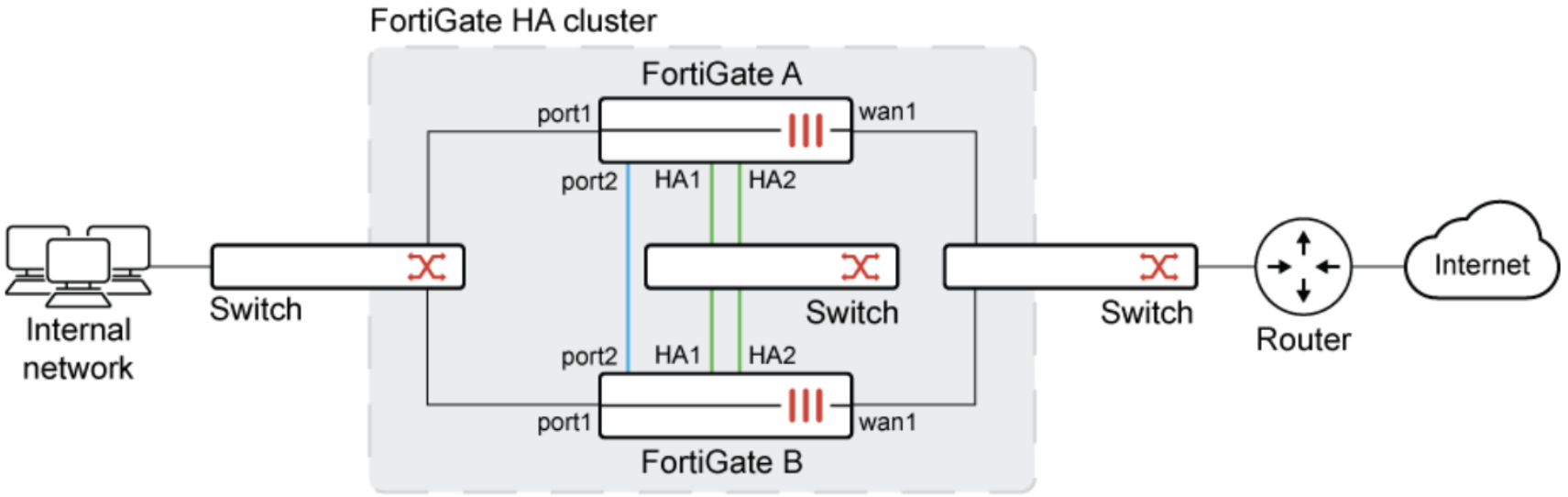
Backup heartbeat interface mitigates split-brain scenarios

Те що Ви так давно просили

Example

In this example, the FortiGate HA cluster consists of two FortiGates (FortiGate A and FortiGate B) connected by two heartbeat interfaces (HA1 and HA2). A backup heartbeat interfaces (port2) is configured too.

Because a backup heartbeat interface is configured, the HA cluster continues to work when heartbeat interfaces HA1 and HA2 are down.



[Backup heartbeat interface mitigates split-brain scenarios | FortiGate / FortiOS 7.6.0 | Fortinet Document Library]

Set the source interface for syslog and NetFlow settings

Контроль надсилання логів та статистики трафіку

FortiOS supports setting the source interface when configuring syslog and NetFlow. This allows syslog and NetFlow to utilize the IP address of the specified interface as the source when sending out the messages. It also simplifies changing the source IP address when an interface IP address is updated or the IP address from a different interface is used. The process becomes more efficient and less time consuming, especially when managing many remote locations.

```
config log syslogd setting
    set status enable
    set source-ip-interface <name>
end

config system netflow
    config collectors
        edit <id>
            set source-ip-interface <name>
        next
    end
end
```

[Set the source interface for syslog and NetFlow settings | FortiGate / FortiOS 7.6.0 | Fortinet Document Library]

Logging detection of duplicate IPv4 addresses

Розслідування IP конфліктів

When enabled, FortiOS can now log each detection of duplicate IPv4 addresses on physical interfaces and VLAN interfaces in the event log under the new log ID 32701. Previously, detection of duplicate IPv4 addresses was not logged. This feature also supports a new SNMP event and new diagnose commands.

The `config system global` command includes a new option:

```
config system global
    set ip-conflict-detection {enable | disable}
end
```

`set ip-conflict-detection {enable | disable}`	Enable/disable logging of IPv4 address conflict detection.

[Logging detection of duplicate IPv4 addresses | FortiGate / FortiOS 7.6.0 | Fortinet Document Library]

Важливі обмеження

УВАГА. Філіальні моделі.

SSL VPN removed from 2GB RAM models for tunnel and web mode

Обмеження для «маленьких» моделей

On FortiGate models with 2GB of RAM or below, the SSL VPN web and tunnel mode feature will no longer be available from the GUI or CLI. Settings will not be upgraded from previous versions.

The affected models include:

- FGT-40F/FWF-40F and variants
- FGT-60F/FWF-60F
- FGT-61F/FWF-61F
- FGR-60F and variants (2GB versions only)

To confirm if your FortiGate model has 2 GB RAM, enter `diagnose hardware sysinfo conserve` in the CLI and check that the total RAM value is below 2000 MB (1000 MB = 1 GB).

On these FortiGate models, consider migrating to using IPsec Dialup VPN for remote access.

See SSL VPN to IPsec VPN Migration for more information.

SSL VPN removed from 2GB RAM models for tunnel and web mode | FortiGate / FortiOS 7.6.0 | Fortinet Document Library

2 GB RAM FortiGate models no longer support FortiOS proxy-related features

Обмеження для «маленьких» філіальних моделей

After upgrade to FortiOS 7.4.4 or later, the following proxy features are no longer supported on impacted devices:

- Zero Trust Network Access (ZTNA)
- UTM profile with proxy-based inspection mode
- Firewall policy with proxy-based inspection mode
- Explicit and transparent proxies
- Virtual server load balance
- Proxy-only UTM profiles:
  - Video Filter
  - Inline CASB
  - ICAP
  - Web application firewall (WAF)
  - SSH Filter
- WAN optimization

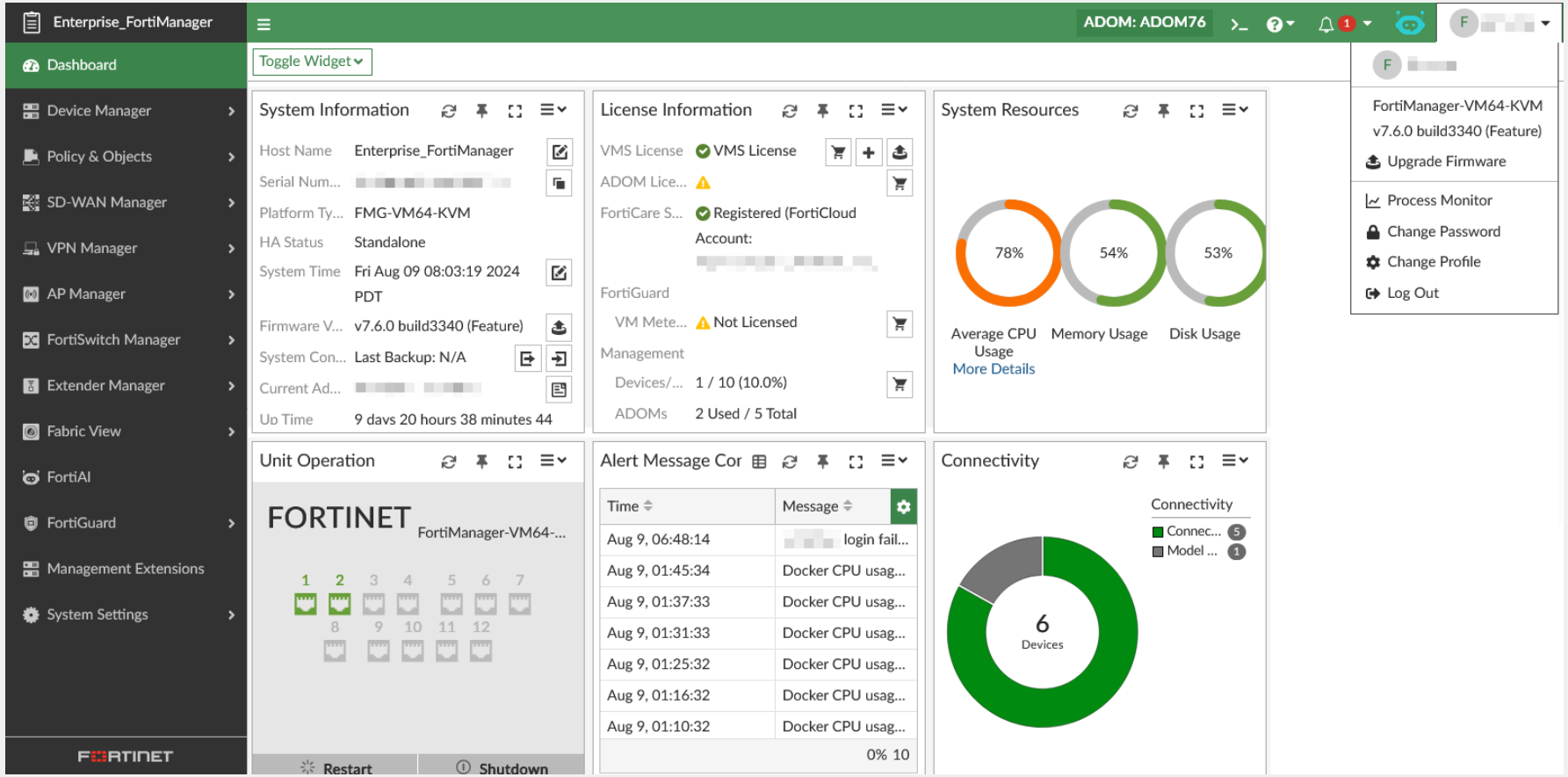
Proxy-related features no longer supported on FortiGate 2 GB RAM models 7.4.4 | FortiGate / FortiOS 7.4.0 | Fortinet Document Library

FortiAnalyzer та FortiManager

Куди ж без них

FortiManager introduces OS firmware levels Feature(F) and Mature(M)

Так само як в FortiGate

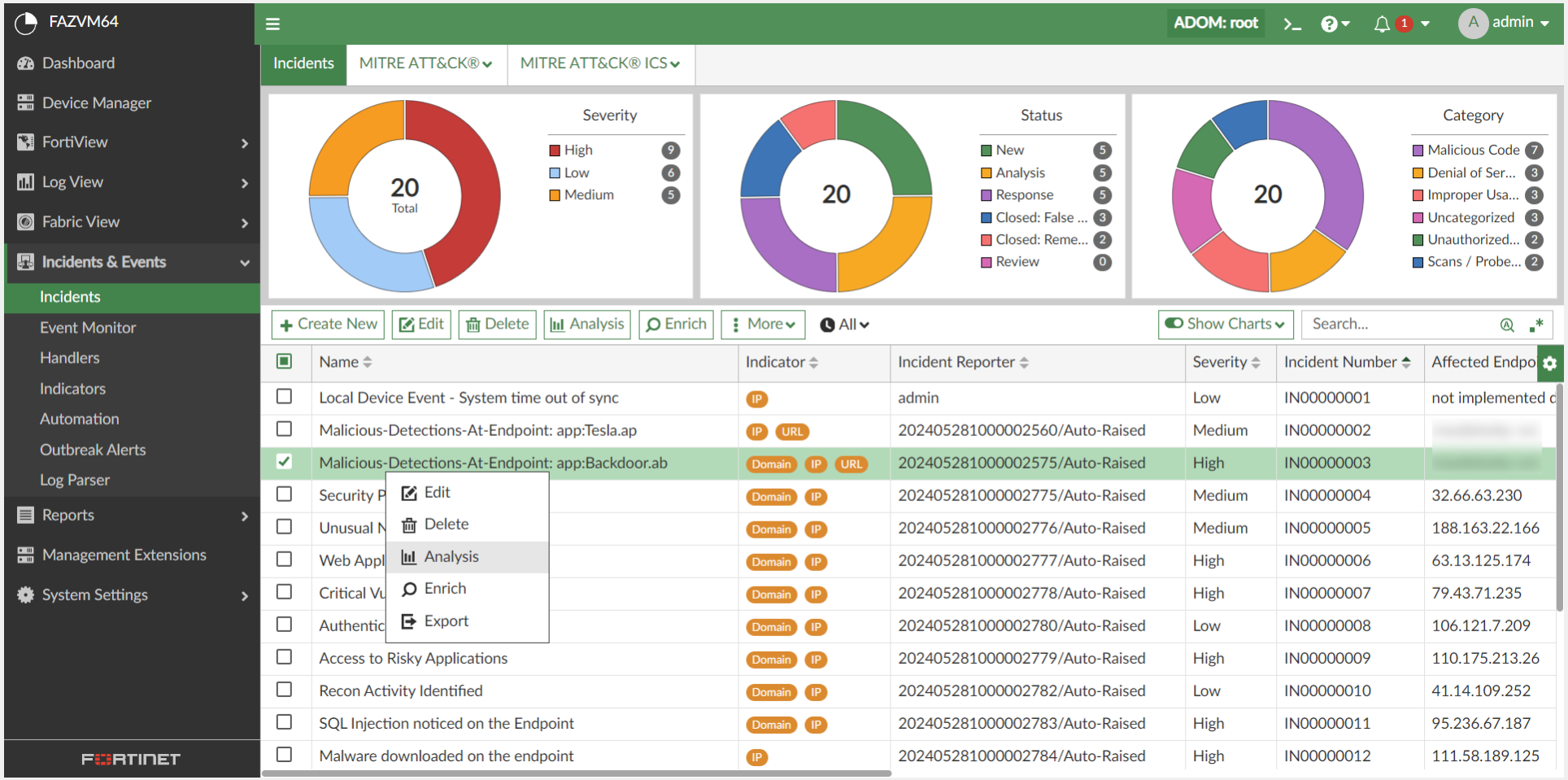


[FortiManager introduces OS firmware levels Feature(F) and Mature(M) | FortiManager 7.6.0 | Fortinet Document Library]

[FortiAnalyzer introduces OS firmware levels Feature(F) and Mature(M) | FortiAnalyzer 7.6.0 | Fortinet Document Library]

Incident analysis re-design

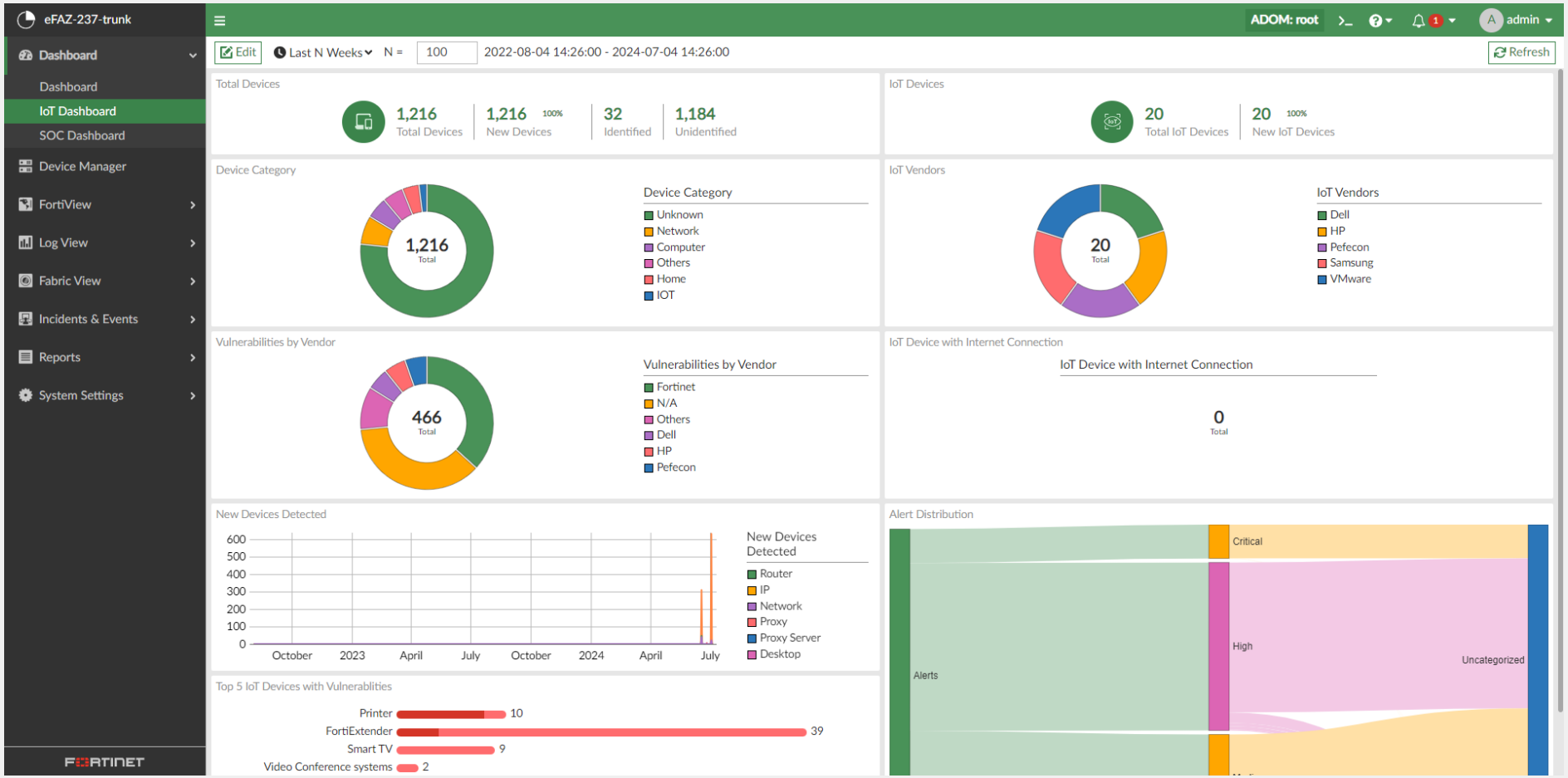
Рухаємось в сторону SOC



[Incident analysis re-design | FortiAnalyzer 7.6.0 | Fortinet Document Library]

IoT dashboard

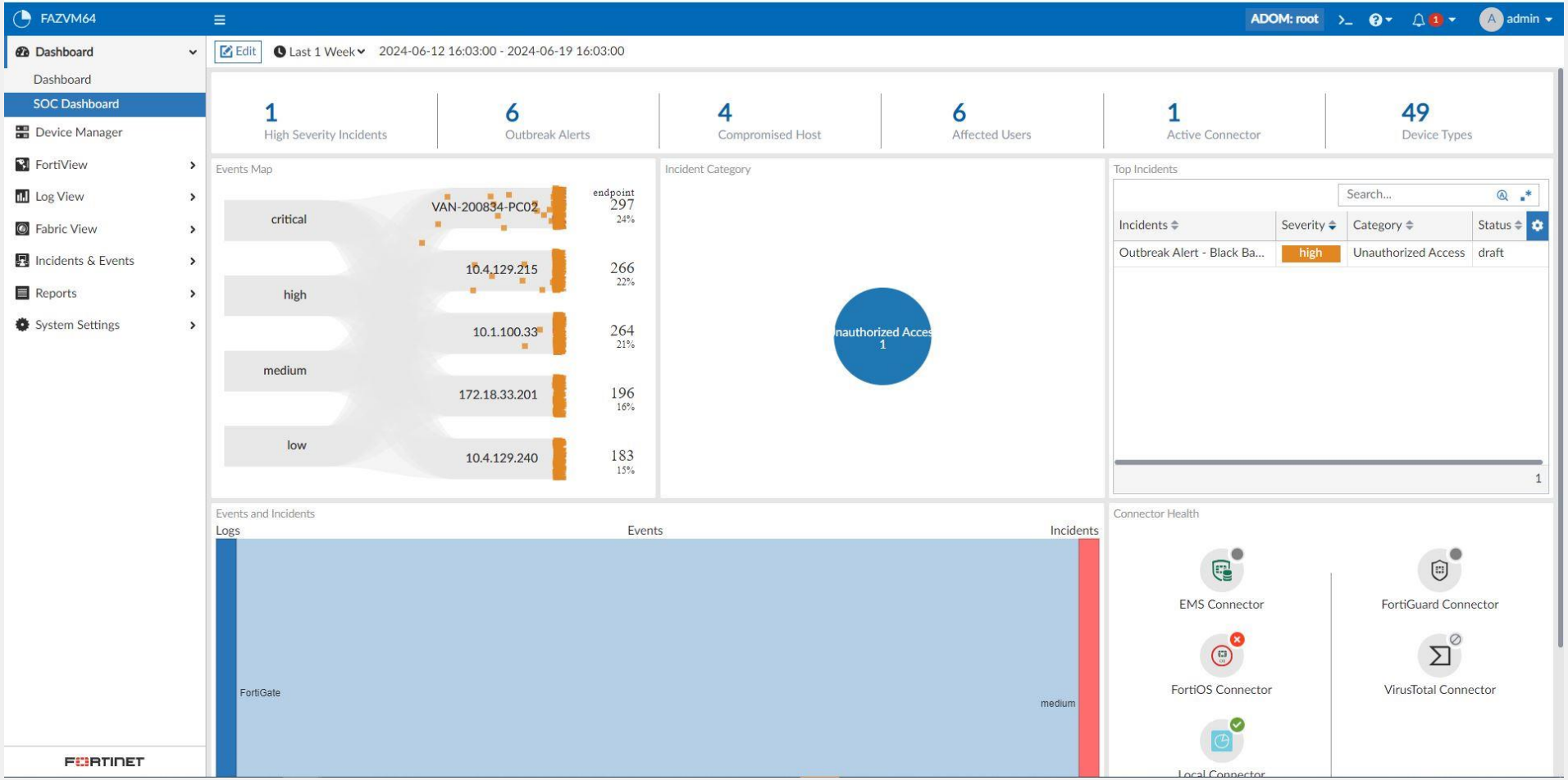
Акцент на IoT



[IoT Dashboard | FortiAnalyzer 7.6.0 | Fortinet Document Library]

Incident analysis re-design

Ще один крок до SOC



[SOC dashboard for alerts and incidents | FortiAnalyzer 7.6.0 | Fortinet Document Library]

FortiAI

в FortiAnalyzer та FortiManager

Час від повного розбору та знешкодження інциденту від 18.5 годин до 10 хвилин.

До

21 Days
(if at all)

12 hrs | 6 hr | 12 hrs

Після

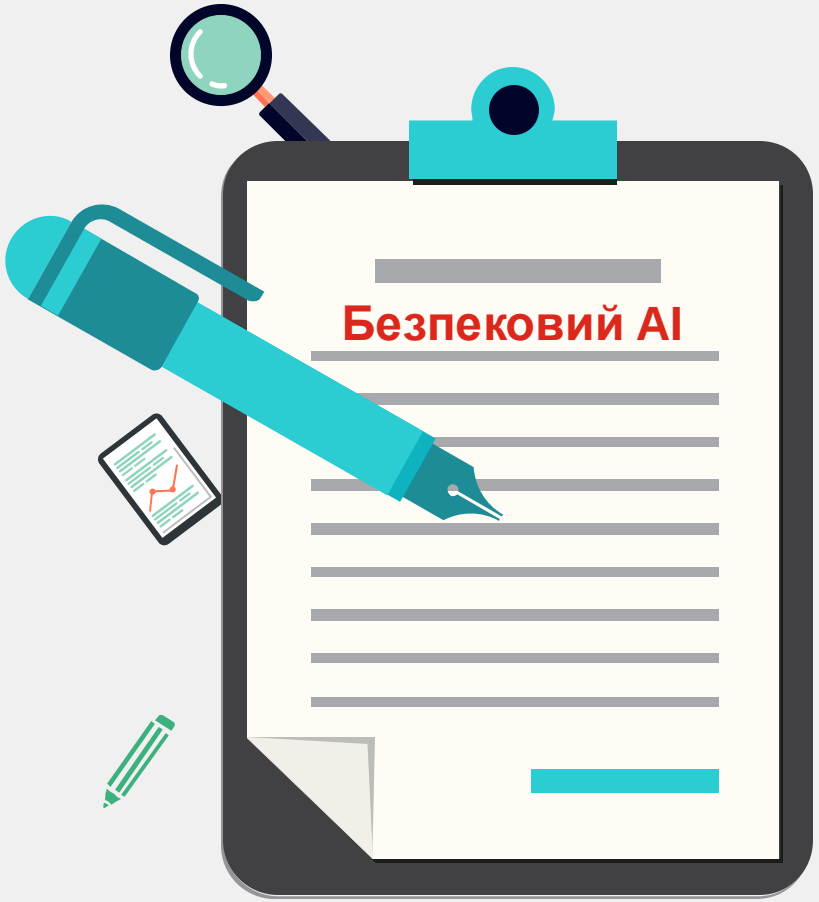
Fortinet SecOps Platform

<1 hr

Виявлення | Ізоляція | Аналіз | Виправлення

Source: Enterprise Strategy Group, a division of Tech Target, Inc.

Бачення FortiAI



Повне використання Fortinet Security Fabric

Використання інтеграції в рамках фабрики для всеохоплюючої роботи

На основі реальних задач

Функціїї та можливості засновані на реальних потребах NOC та SOC

Самонавчання

Покращення ефективності рішень Fortinet у замовників

Автоматизація

Автоматична система що реалізовує потреби і виправляє вразливі місця

Що робить AI?

Видимість

Вивчення IT від мережі, користувачів та сервісів до їх безпекових параметрів.

Прийняття рішень

Рекомендовані дії на основі вивченого та best practice

Впровадження

Автоматизоване застосування рекомендованих дій

Інтуїтивна AI допомога

FortiAI: Вбудовані можливості GenAI для проактивного керування загрозами та автоматизації

Оцінка
Використання FortiAI для пошуку аномалій з усіх наявних даних.

Передбачення
Протидійте порушенням ще до їх виникнення

Best Practices
Постійні поради та рекомендації

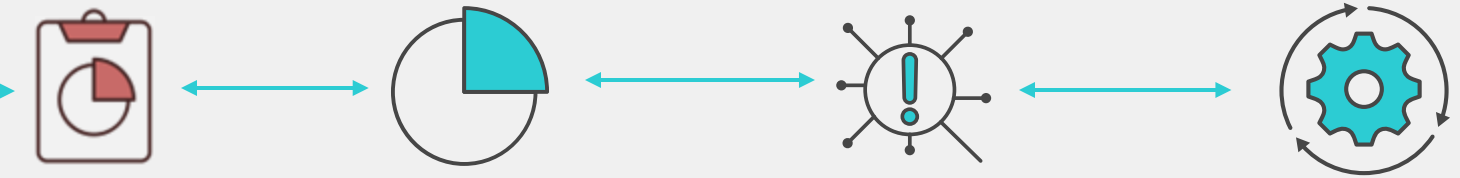
FortiAI

Контекстний GenAI помічник що спрощує та пришвидшує роботу

- Розслідування та відповідь на загрози
- Створення звітів/запитів FortiAnalyzer
- Голосове керування

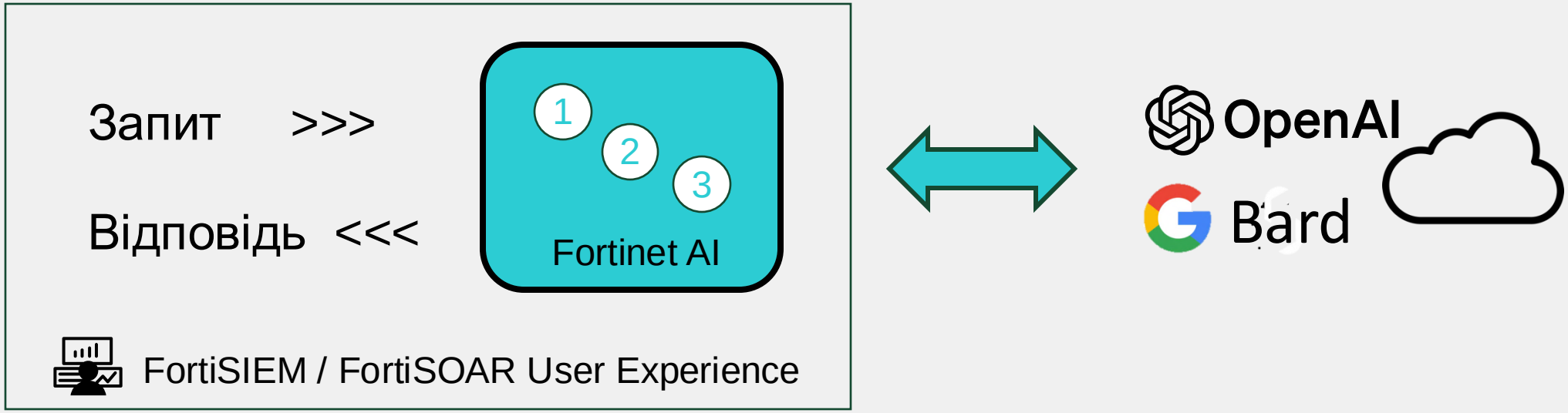
Спілкування «природньою мовою»

”Please analyze the latest security event, provide a detailed summary, assess its potential impact, and suggest appropriate remediation actions”



FortiManager **FortiAnalyzer** **FortiSIEM** **FortiSOAR**

Як працює FortiAI?



1 **Доповнення даних GenAI**

Надає базу даних Fortinet та приклади для механізму AI

2 **Трансформація запиту**

Додає до запиту деталі для правильної AI обробки

3 **Кореляція відповідей**

Створює повну та релевантну відповідь враховуючи уточнення користувача

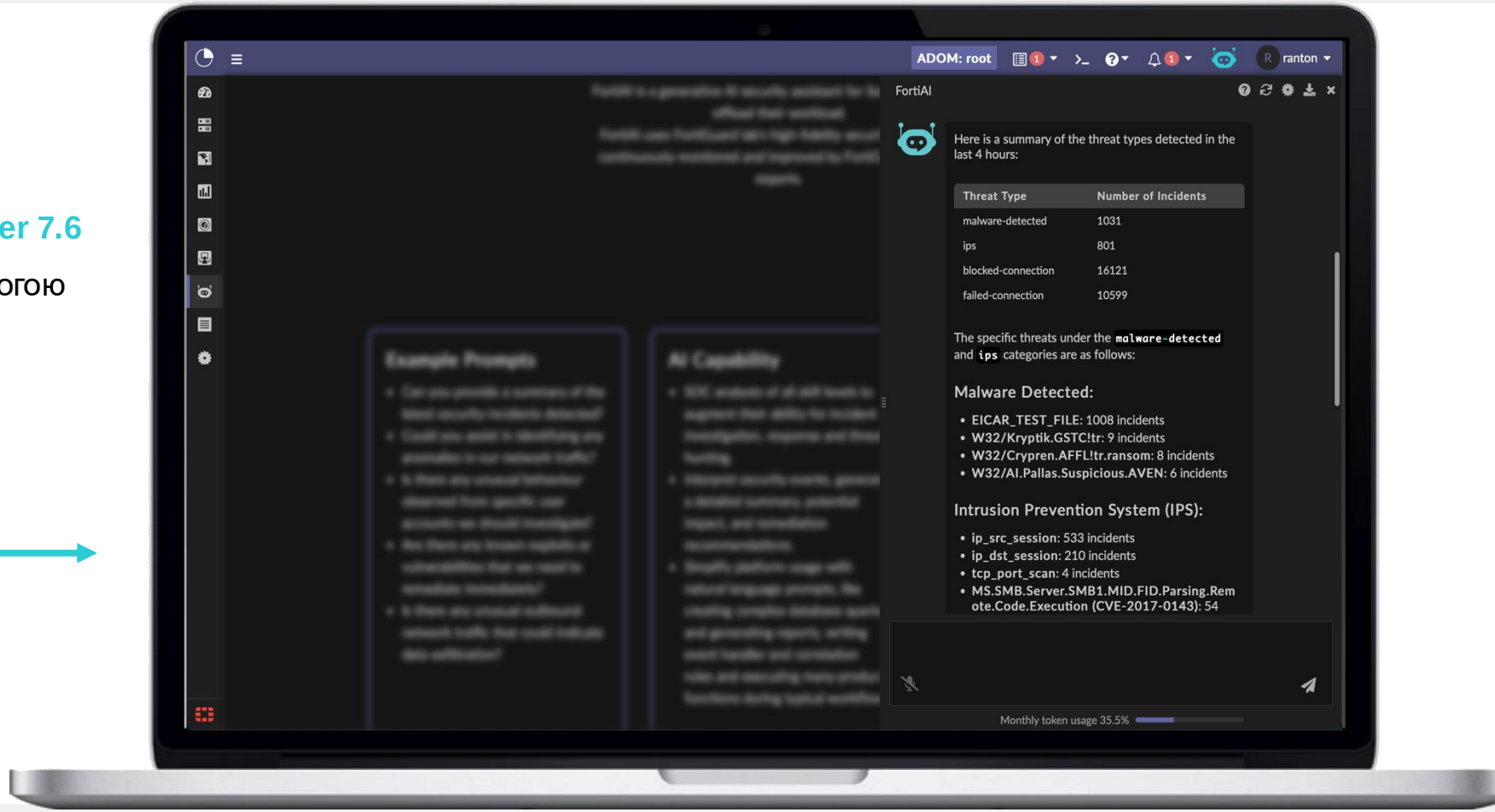
Безпека та приватність

Обмін даними Cloud AI механізму обмежено явним вмістом взаємодії з клієнтом
Критична інформація може бути автоматично замаскована до передачі
Fortinet Advisor не передає дані клієнтів і не надає доступ до них..

FortiAI в FortiAnalyzer

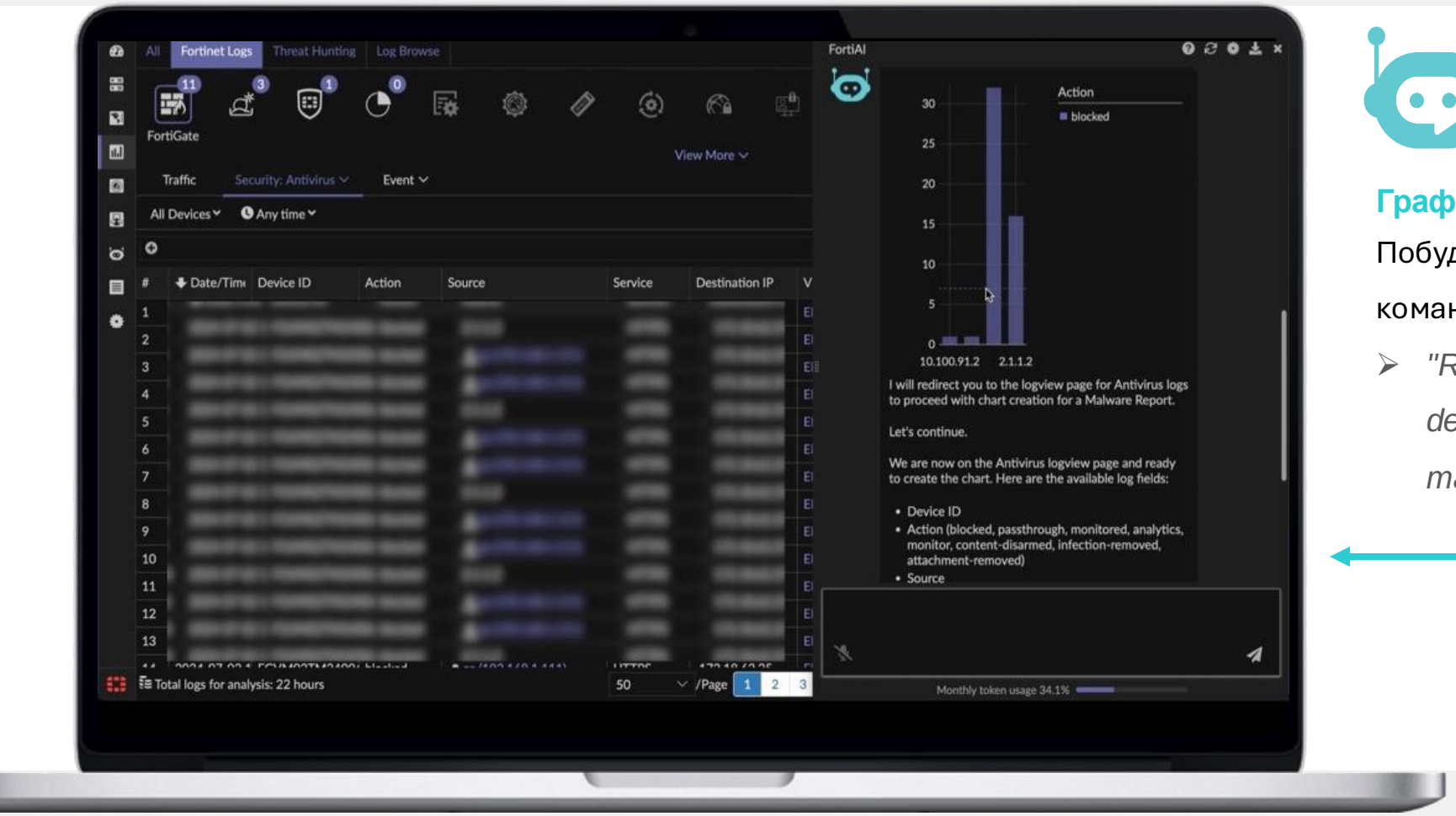
Додаткова ліцензія AI для FortiAnalyzer 7.6

Швидший та простіший аналіз за допомогою допомоги Gen-AI



*FortiAI для FortiAnalyzer потребує окремої ліцензії

FortiAI візуалізація in FortiAnalyzer



Графічна візуалізація

Побудова графіку за допомогою голосової команди.

- *"Render a pie chart for blocked threats by destination IP" or "Show a bar chart of malware activities by threat type"*

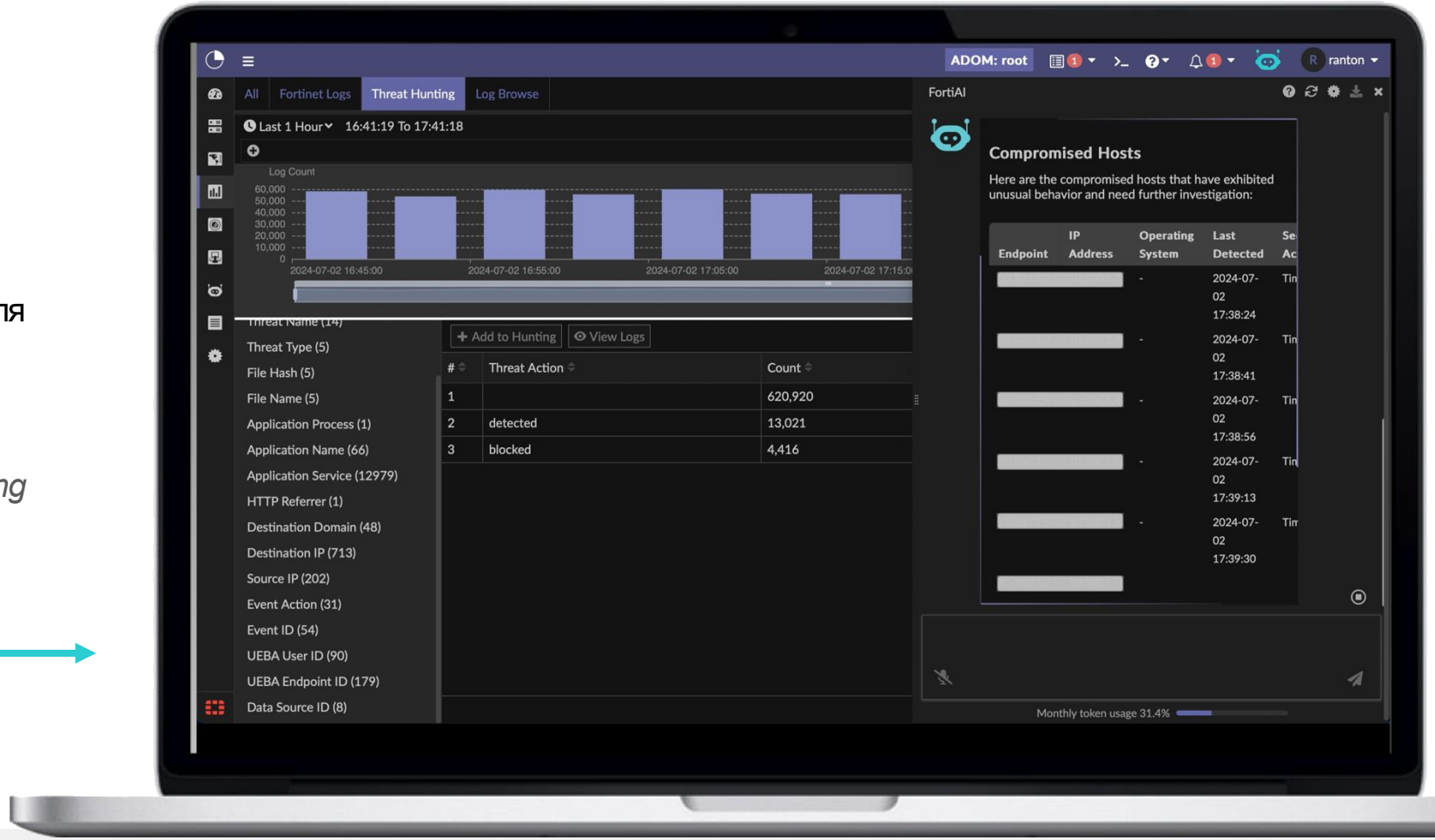
*FortiAI для FortiAnalyzer потребує окремої ліцензії

Пошук загроз з FortiAI засобами FortiAnalyzer

Telemetry Analysis Turns Data into Action

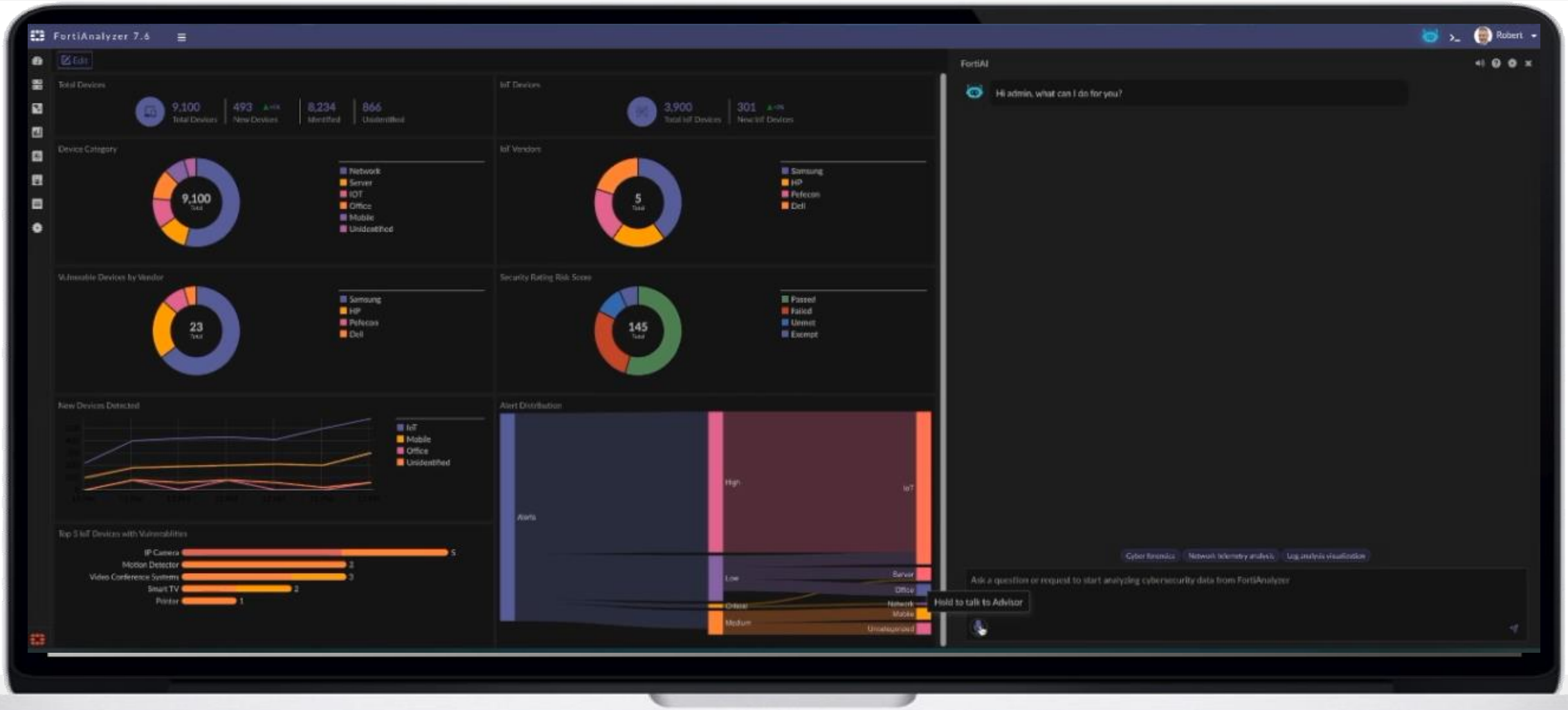
Аналітики можуть використовувати запити для отримання статистики журналів на основі вказаних фільтрів, часу тощо.

- *“Show me threats without blocking happening on risky destinations"*
- *"Give me the statistics of malware activities detected today by threat name"*



*FortiAI для FortiAnalyzer потребує окремої ліцензії

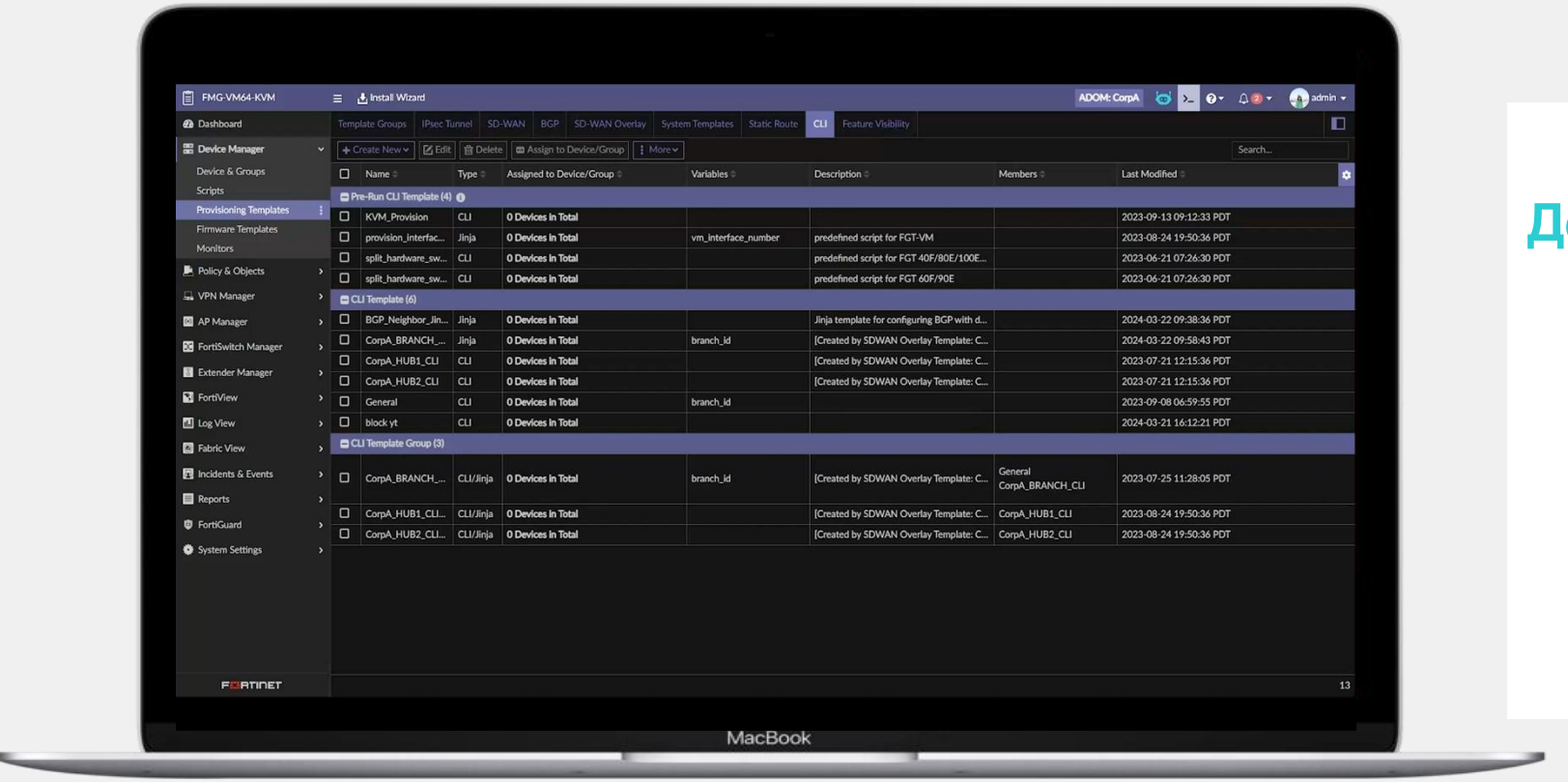
Як це виглядає в роботі FortiAnalyzer?



New

FortiAI для FortiManager

Можливості FortiManager в керуванні мережею та її безпекою



День 0-1: Швидке налаштування

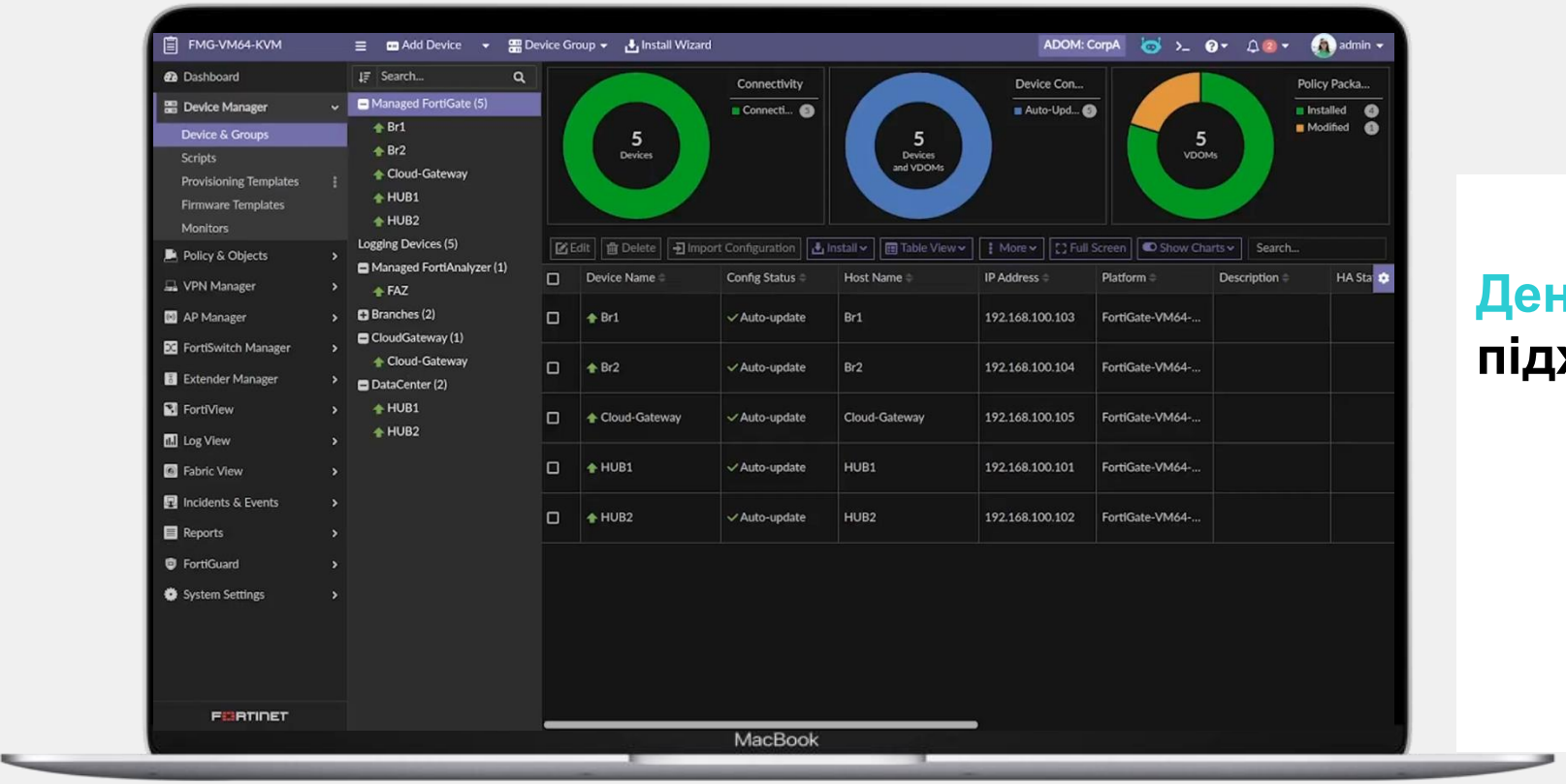
- Допомога зі скриптами
- CLI, Jinja та VPN помічник
- Перевірка та поради
- Збереження скриптів та шаблонів перед запуском

*FortiAI для FortiManager потребує окремої ліцензії

New

FortiAI для FortiManager

Можливості FortiManager в керуванні мережею та її безпекою



День 2: Перехід від реактивного підходу до проактивного:

- Помічник IoT
- Заглиблення у вразливості
- Рекомендовані дії
- Звітність

*FortiAI для FortiManager потребує окремої ліцензії

Кілька AI партномерів для FortiAnalyzer та FortiManager

Одна градація для прикладу

FC1-10-AZVMS-1118-01-12	FortiAnalyzer-VMS **FortiAI Subscription** 1 Year Generative AI powered security service utilizing large language models (LLMs) for real-time assistance in SOC analysis, incident investigation, triage and response (**5 GB/Day of logs**)
FC1-10-FMGVS-1118-01-12	FortiManager-VMS **FortiAI Subscription** 1 Year Generative AI powered central management service, utilizing large language models (LLMs) for real-time assistance in orchestration, automation and monitoring for **10 devices/vdoms**

Ще трохи новин

Останній розділ

SIEM

Нова ліцензійна модель на основі Gb/day. Одна градація для прикладу.

FC1-10-SMGS1-1026-02-12	FortiSIEM GB Subscription License 1 Year FortiSIEM Subscription license for 40GB - 99GB Logs per day. Increments of additional 1GB Logs per day. Includes HA Super, FortiCare Premium support.
FC1-10-SMGS1-334-02-12	FortiSIEM GB UEBA Subscription License 1 Year Per UEBA Agent based telemetry Subscription License for 25 - 499 Agents
FC1-10-SMGS1-182-02-12	FortiSIEM GB Advanced Agent Subscription License 1 Year Per Agent Subscription License for 25 - 499 Agents. Providing File Integrity Monitoring (Windows, Linux), log & performance monitoring
FC1-10-SMGS1-149-02-12	FortiSIEM GB Indicators of Compromise (IOC) Service 1 Year FortiGuard Indicators of Compromise (IOC) Service (for 1 - 50GB/Day of Logs)

FortiEndpoint

Обіцяна уніфікація агенту

FC1-10-EMS05-1045-02-12	FortiEndpoint - **Zero Trust** Connect 1 Year FortiEndpoint - Zero Trust (ZTNA/VPN) Subscription including FortiCare Premium for 25-49 Endpoints.
FC1-10-EMS05-1046-02-12	FortiEndpoint - **Prevent** 1 Year FortiEndpoint - Advanced EPP (with ZTNA/VPN) including FortiCare Premium for 25-49 Endpoints.
FC1-10-EMS05-1047-02-12	FortiEndpoint - **Prevent + SOC** 1 Year FortiEndpoint - Advanced EPP (with ZTNA/VPN) plus FortiGuard Forensics and SOCaaS integration, including FortiCare Premium for 25-49 Endpoints.
FC1-10-EMS05-1040-02-12	FortiEndpoint - **XDR** 1 Year FortiEndpoint - XDR Essentials Subscription (Discover & Protect) with ZTNA/VPN + Advanced EPP including FortiCare Premium for 25-49 Endpoints.
FC1-10-EMS05-1041-02-12	FortiEndpoint - **XDR AI** 1 Year FortiEndpoint - XDR AI Subscription (Discover, Protect & Respond) with XDR-AI, ZTNA/VPN and Advanced EPP including FortiCare Premium for 25-49 Endpoints.
FC1-10-EMS05-1042-02-12	FortiEndpoint - **XDR AI + SOC** 1 Year FortiEndpoint - XDR Complete Subscription (Discover, Protect & Respond) with XDR-AI, ZTNA/VPN and Advanced EPP, plus FortiGuard Forensics and SOCaaS integration, including FortiCare Premium for 25-49 Endpoints.

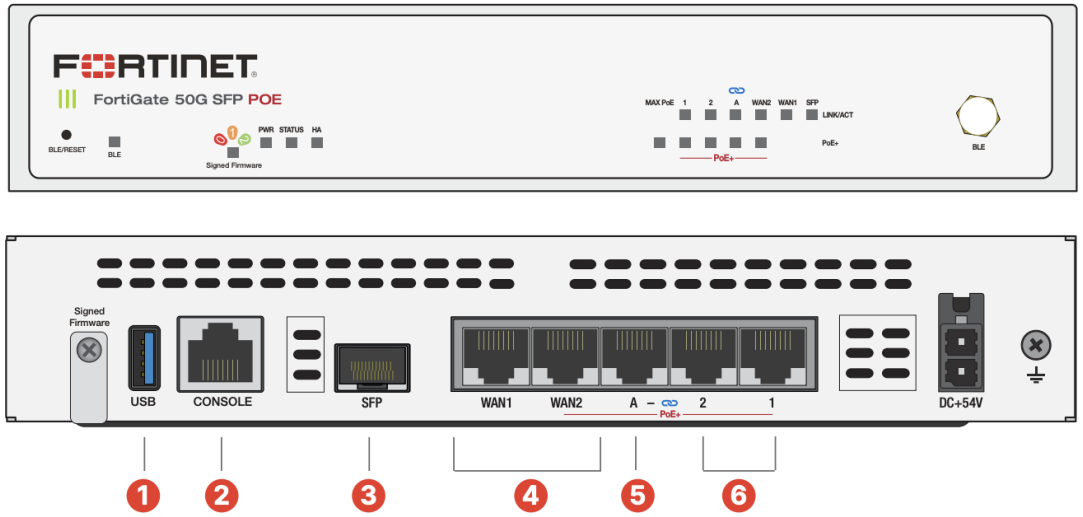
FortiGate 50G

FG-50G-DSL, FG-50G-SFP, FG-50G-SFP-PoE, FG-51G-SFP-POE, FWF-50G-DSL, FWF-50G-SFP

FortiGate 50/51G-SFP-POE

SP5 | TPM

DESKTOP | GE | SFP | POE | 64GB



Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 1 x GE SFP Port
4. 2 x GE RJ45 WAN Ports (WAN2 PoE+)
5. 1 x GE RJ45 FortiLink Port (PoE+)
6. 2 x GE RJ45 Ethernet Ports (PoE+)

IPS	NGFW	Threat Protection	Interfaces
2.25 Gbps	1.25 Gbps	1.1 Gbps	Multiple GE RJ45 | Variants with 5G, PoE, DSL, SFP, WiFi, and/or storage

[FortiGate FortiWiFi 50G Series Data Sheet (fortinet.com)]

FortiGate 30G

Заміна для «найменших» з F серії.

FG-30G	FortiGate-30G 4 x GE RJ45 ports (including 3 x Internal Ports, 1 x WAN Ports)

Дякую за Ваш час та увагу

Q&A

ytaran@fortinet.com