Ochrona przed głównymi wektorami cyberataku przy użyciu rozwiązań Fortinet

Andrzej Suski

Technical Solutions Engineer – Arrow ECS

Obszary i wyzwania dla cyberbezpieczeństwa

Użytkownicy & Urządzenia

Transport 

Praca Dom 

Biuro 

Sieci

Wi-Fi 

Switch 

SD-WAN 

5G 

Aplikacje

Cloud 

Data Center 

Dane na Serwerach 

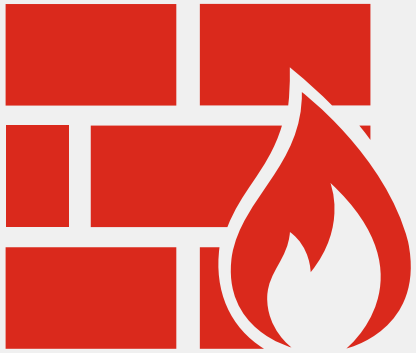
Wykorzystanie e-maila jako głównego wektora zagrożeń

Ransomware, wzrost około 10% roku do roku.

Średni koszt pojedynczego ataku.

*Statistics from Verizon Data Breach Investigations Report 2021.
**Ponemon Institute Cost of a Data Breach Report 2020.

Co można zrobić by zabezpieczyć dane?



Firewall

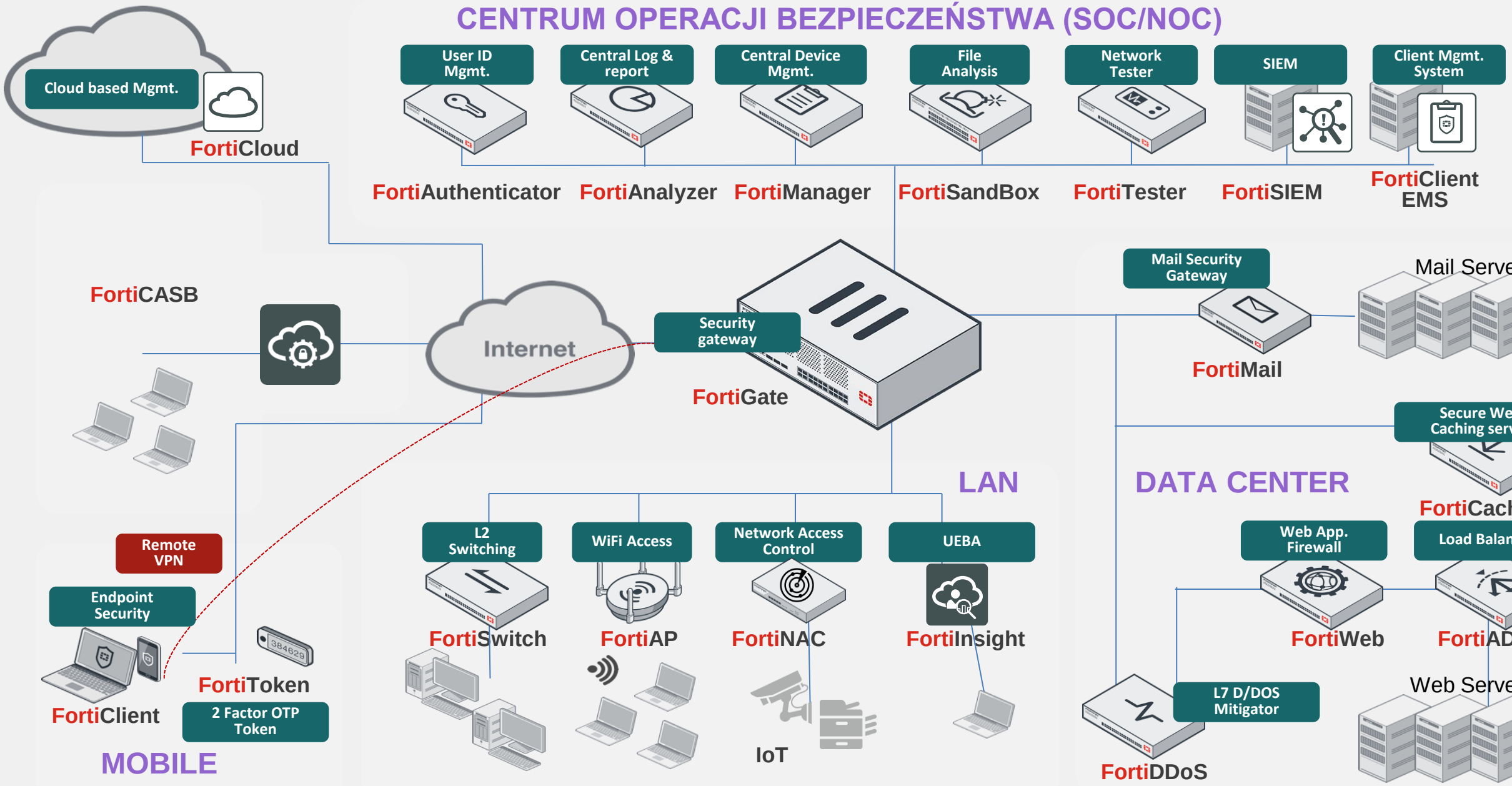
Hasła / Klucze

Szyfrowanie VPN

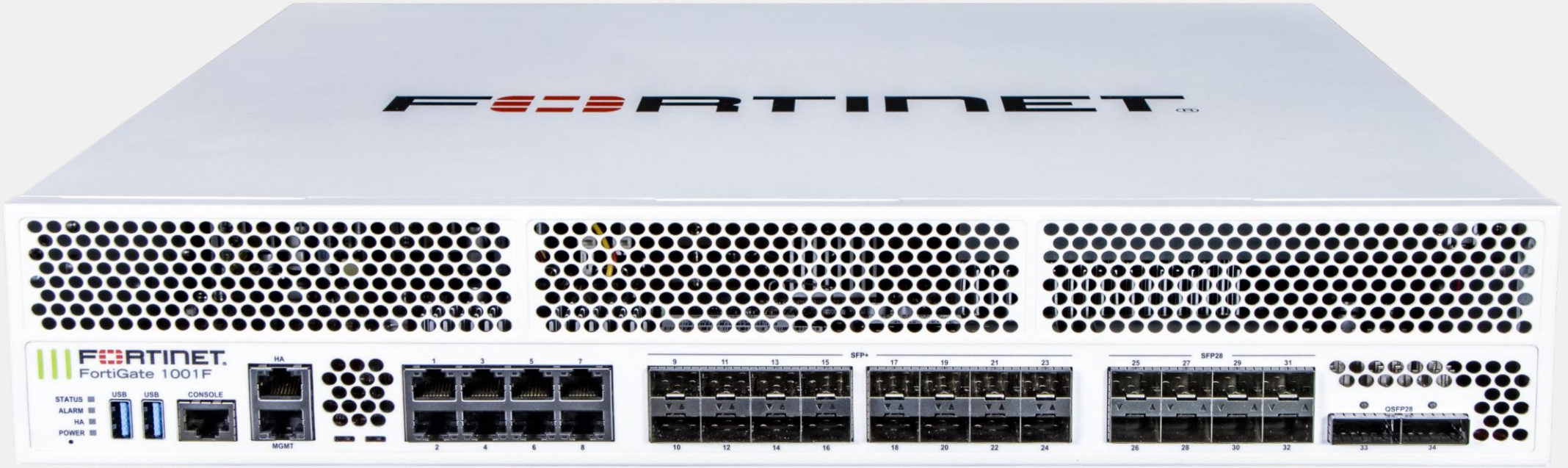
Antyvirus Antyspam

Zintegrowany System Bezpieczeństwa

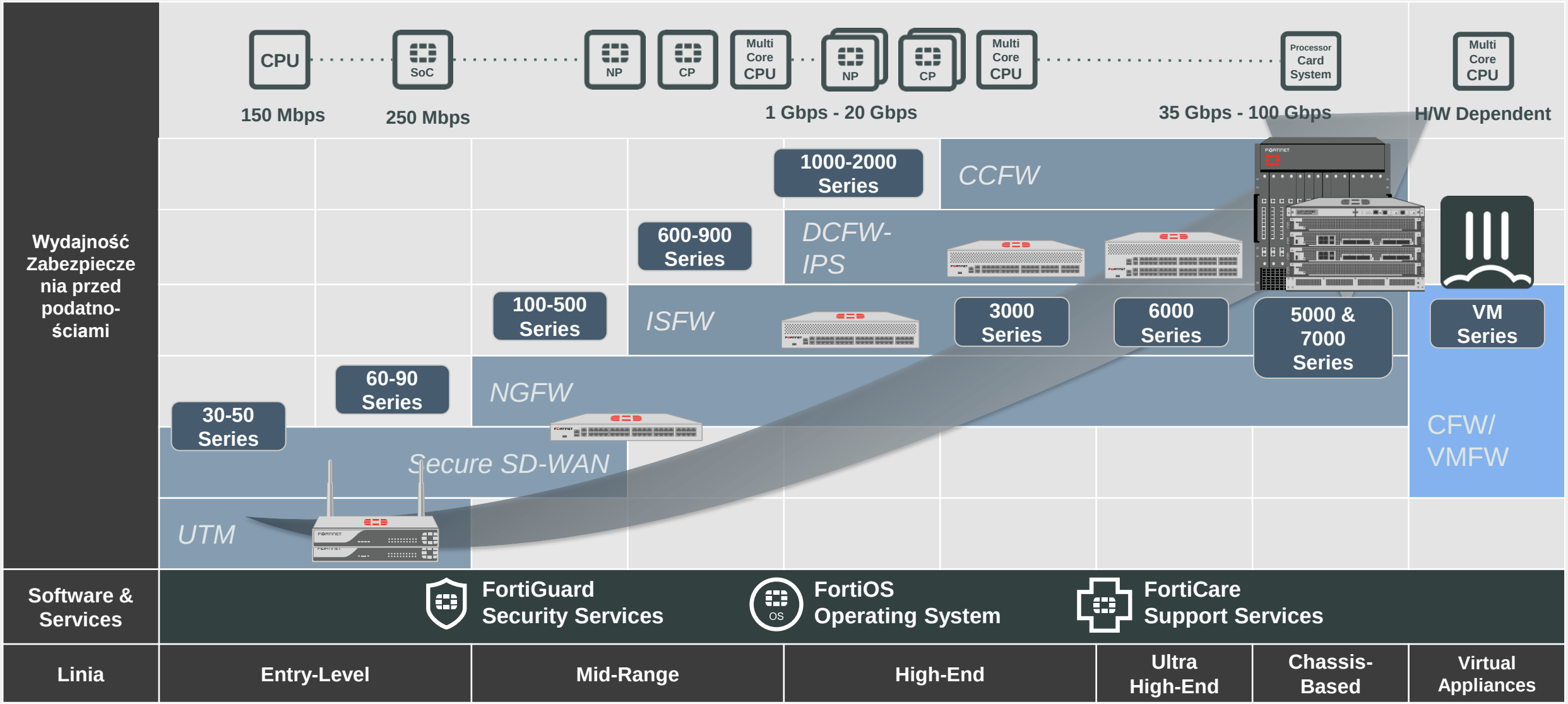
CENTRUM OPERACJI BEZPIECZEŃSTWA (SOC/NOC)



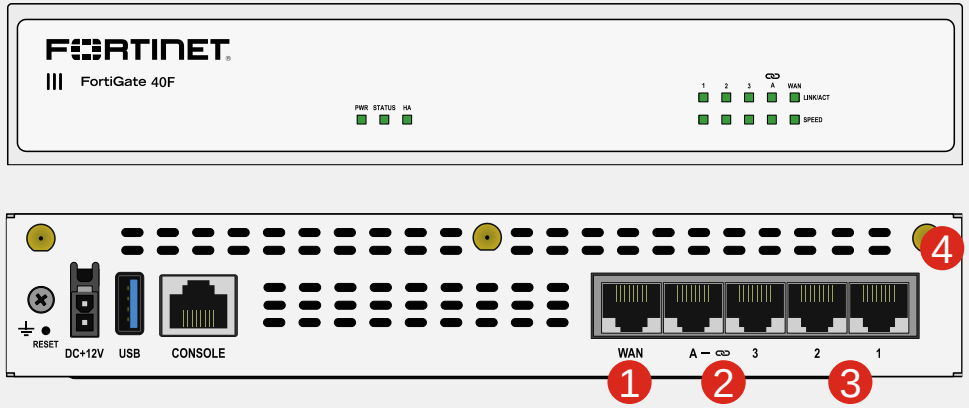
Fortinet Fortigate – Next Generation Firewall



FortiGate Linie Produktowe



FortiGate/FortiWiFi 40F



1. 1 x GE RJ45 Port WAN
2. 1 x GE RJ45 Port FortiLink
3. 3 x GE RJ45 Porty
4. WiFi Variant: 802.11a/b/g/n/ac W2

5 Gbps
Przepływność Firewalla

35,000
Nowe sesje/Sec

700,000
Równoległe sesje

310 Mbps
Przepływność inspekcji SSL

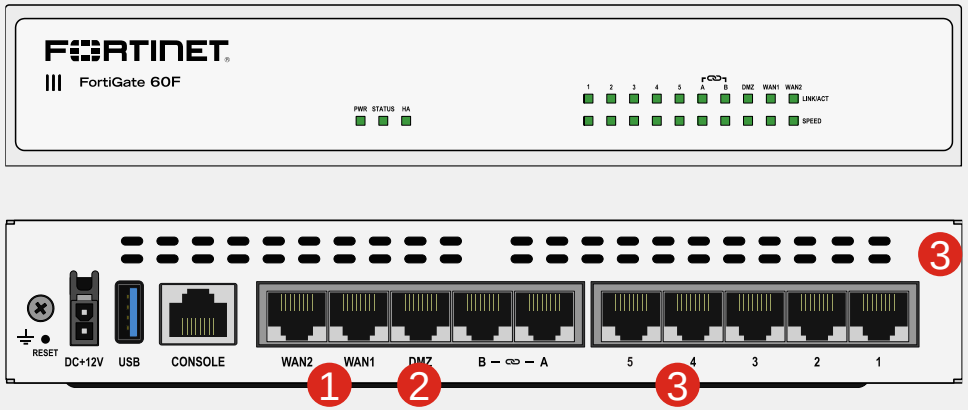
1 Gbps
Przepływność IPS

800 Mbps
Przepływność NGFW

600 Mbps
Przepływność Threat Protection

Małe przedsiębiorstwa
NGFW / Bezpieczny SD-WAN

FortiGate/FortiWiFi 60/61F



1. 2 x GE RJ45 Porty WAN
2. 1 x GE RJ45 Port DMZ
3. 7 x GE RJ45 Portów

10 Gbps
Przepływność Firewalla

1.4 Gbps
Przepływność dla IPS

35,000
Nowe Sesje/Sec

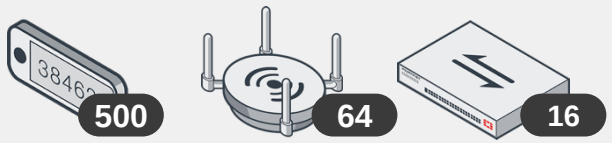
700,000
Jednoczesne Sesje

1. Gbps
Przepływność NGFW

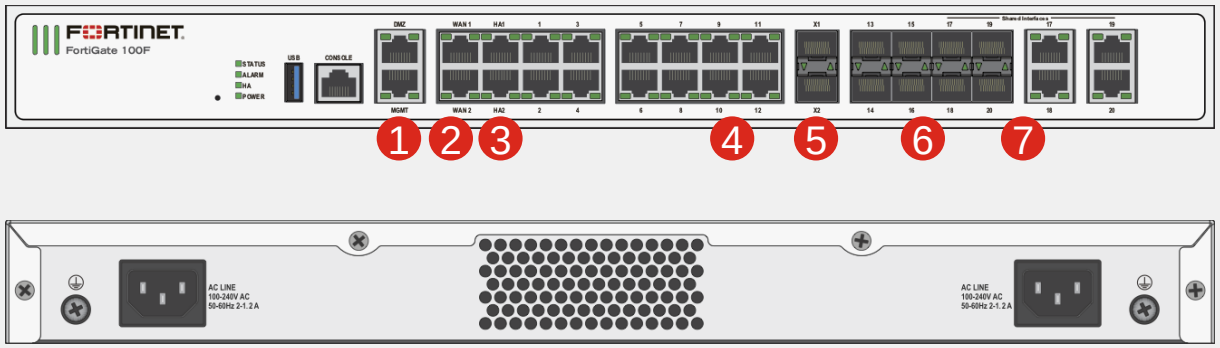
630 Mbps
Przepływność inspekcji SSL

700 Mbps
Przepływność Threat Protection

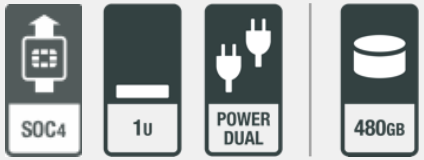
Małe przedsiębiorstwa
NGFW / Bezpieczny SD-WAN



FortiGate 100/101F



1. 2 x GE RJ45 Porty MGMT/DMZ
2. 2 x GE RJ45 Porty HA
3. 2 x GE RJ45 Porty WAN
4. 12 x GE RJ45 Portów
5. 2 x 10GE SFP+ FortiLink porty
6. 8 x GE SFP Portów
7. 4 x GE RJ45/SFP wymienne porty



20 Gbps
Firewall throughput

2.6 Gbps
Przepływność IPS

56,000
Nowe Sesje/Sec

1.5 Million
Sesje Równoległe

1.6 Gbps
Przepływność NGFW

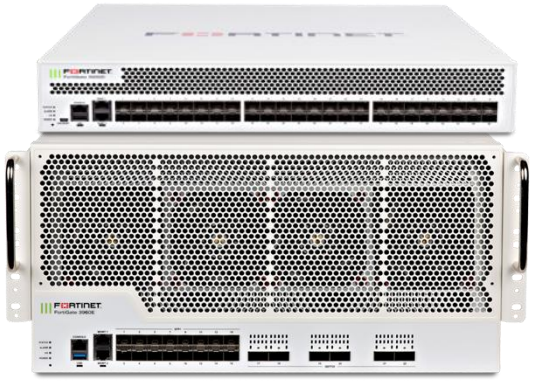
1 Gbps
Przepływność inspekcji SSL

1 Gbps
Przepływność Threat Protection

Średnie przedsiębiorstwa
NGFW / Bezpieczny SD-WAN

Seria FortiGate High End

Data Center Firewall dla dużych przedsiębiorstw z interfejsami o wysokich przepływnościach



- Seria FG-3000 F
- Seria FG-2000 F
- Seria FG-1000 F

NGFW, IPS

Segmentation

SWG

Mobile Security

52 Gbps – 320 Gbps
Przepływność Firewall

5 Gbps – 40 Gbps
Przepływność NGFW

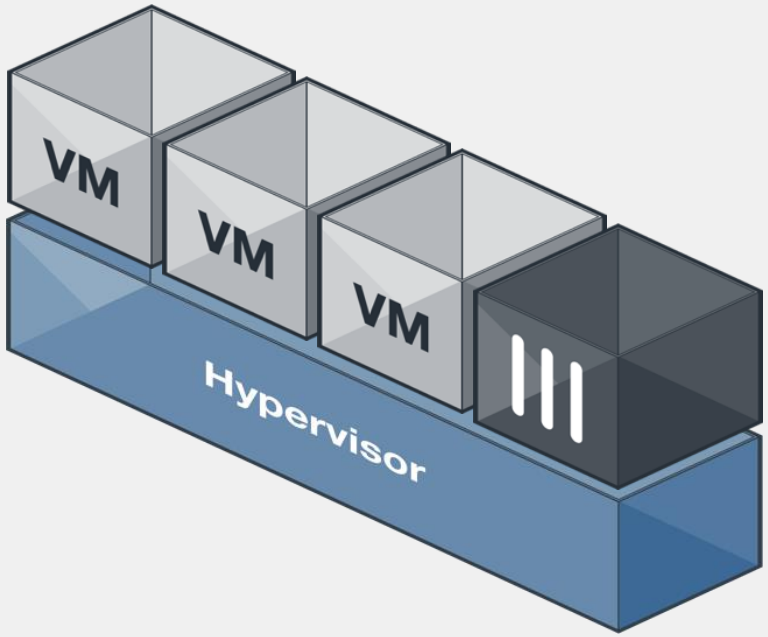
6 Gbps – 55 Gbps
Przepływność IPS

3 Gbps – 30 Gbps
Przepływność Threat Protection

GE RJ45 | GE SFP
10GE SFP+
25GE SFP28
40GE QSFP+
100GE QSFP28

FortiGate - wersja wirtualna (VM)

Bezpieczeństwo dla środowisk wirtualnych



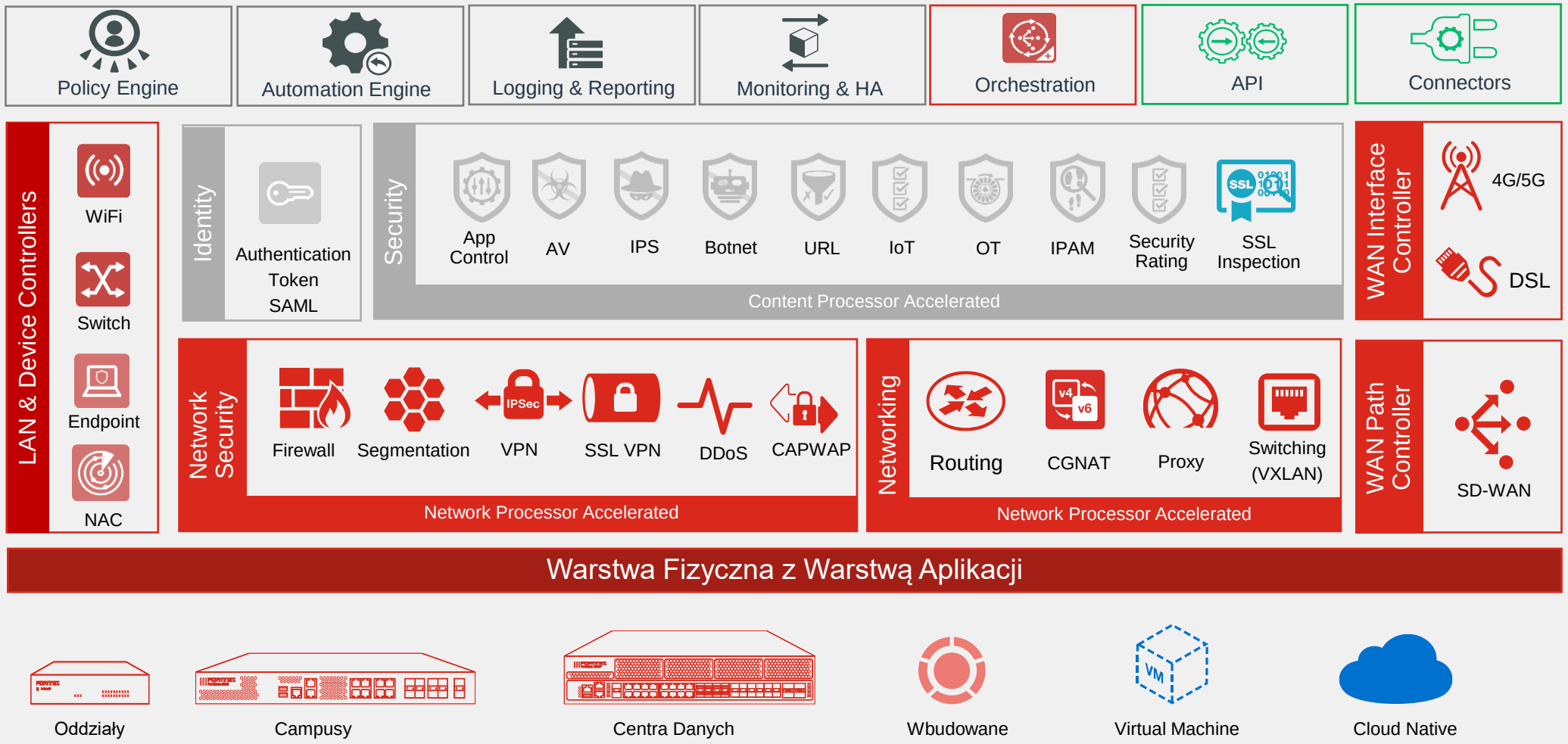
FG-VM

Najważniejsze korzyści:

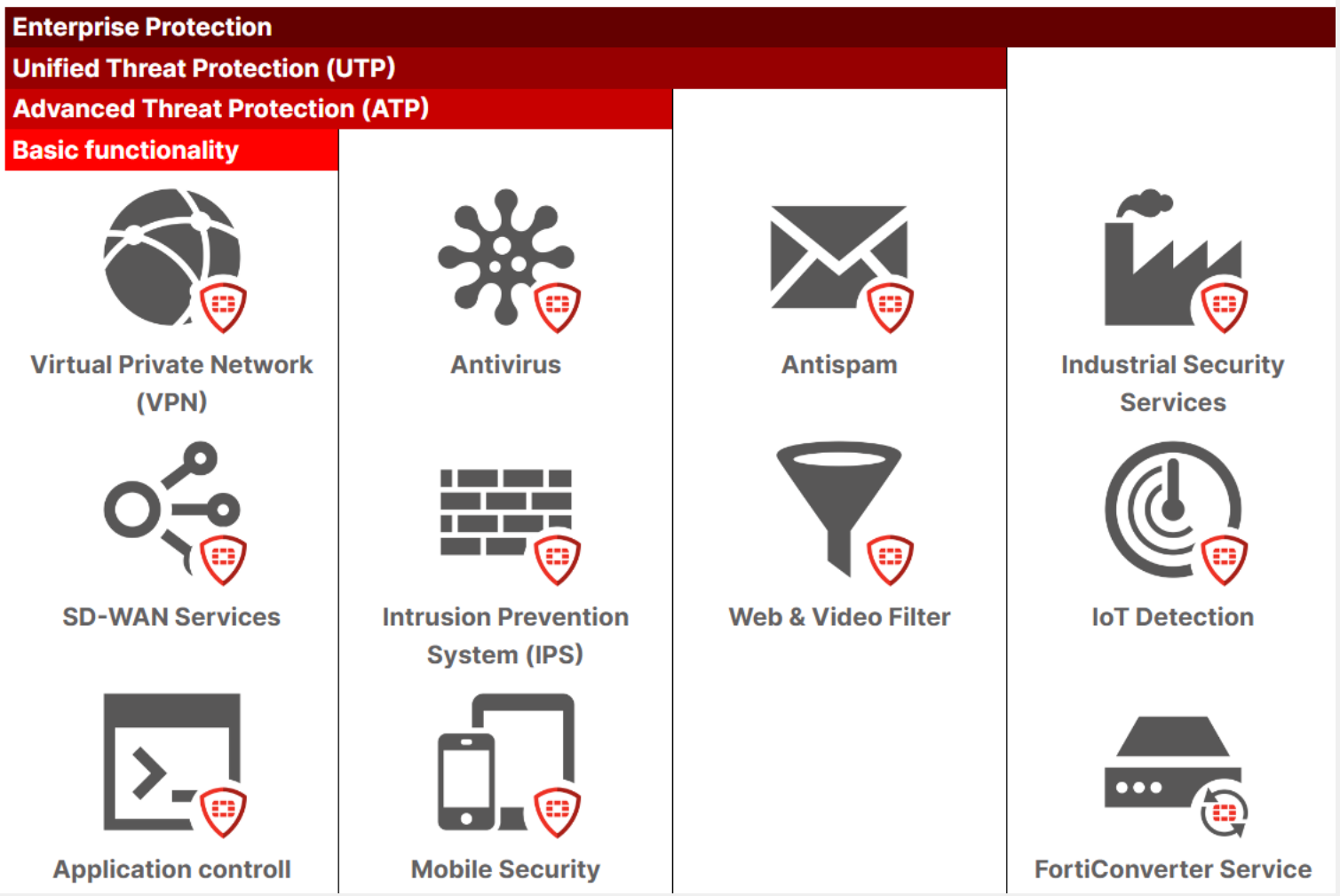
- ✓ Pogłębione bezpieczeństwo i widoczność krytycznych zasobów środowisk wirtualnych
- ✓ Możliwość zarządzania środowiskiem klasycznym i zwirtualizowanym z użyciem tych samych narzędzi zastosowaniem tych samych zasad, reguł i polityk
- ✓ Obsługa różnorodnych hypervisorów
- ✓ Bogaty zestaw funkcji sieciowych i bezpieczeństwa pozwalający na wdrożenia dowolnej skali (geograficznej i funkcjonalnej)

VMware ESXi | Citrix Xen | Xen | KVM | MS Hyper-V | Amazon AWS | MS Azure | GCP

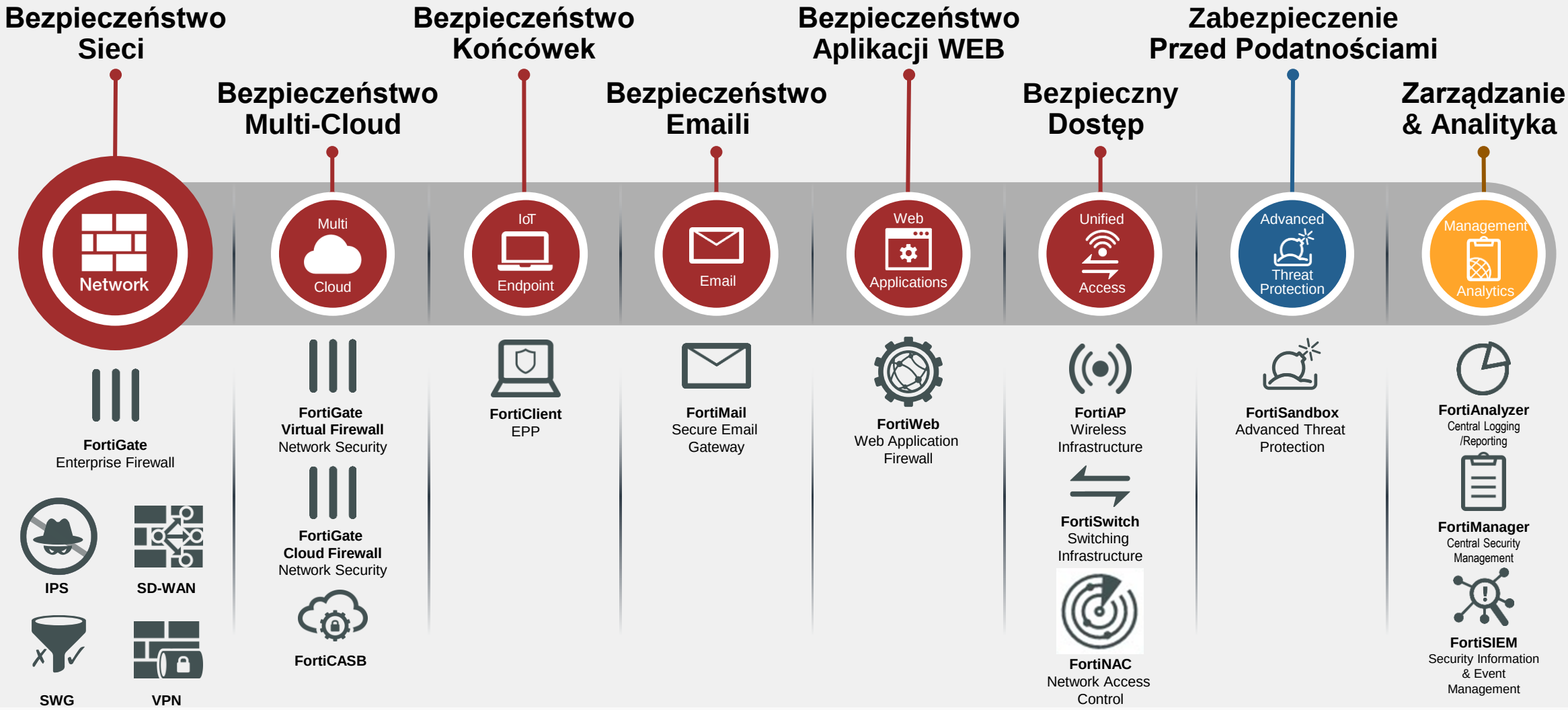
FortiOS Innowacyjny System Bezpieczeństwa Sieciowego



Licencja i jej elementy



Komponenty i koncepcja Fortinet Security Fabric



FortiManager

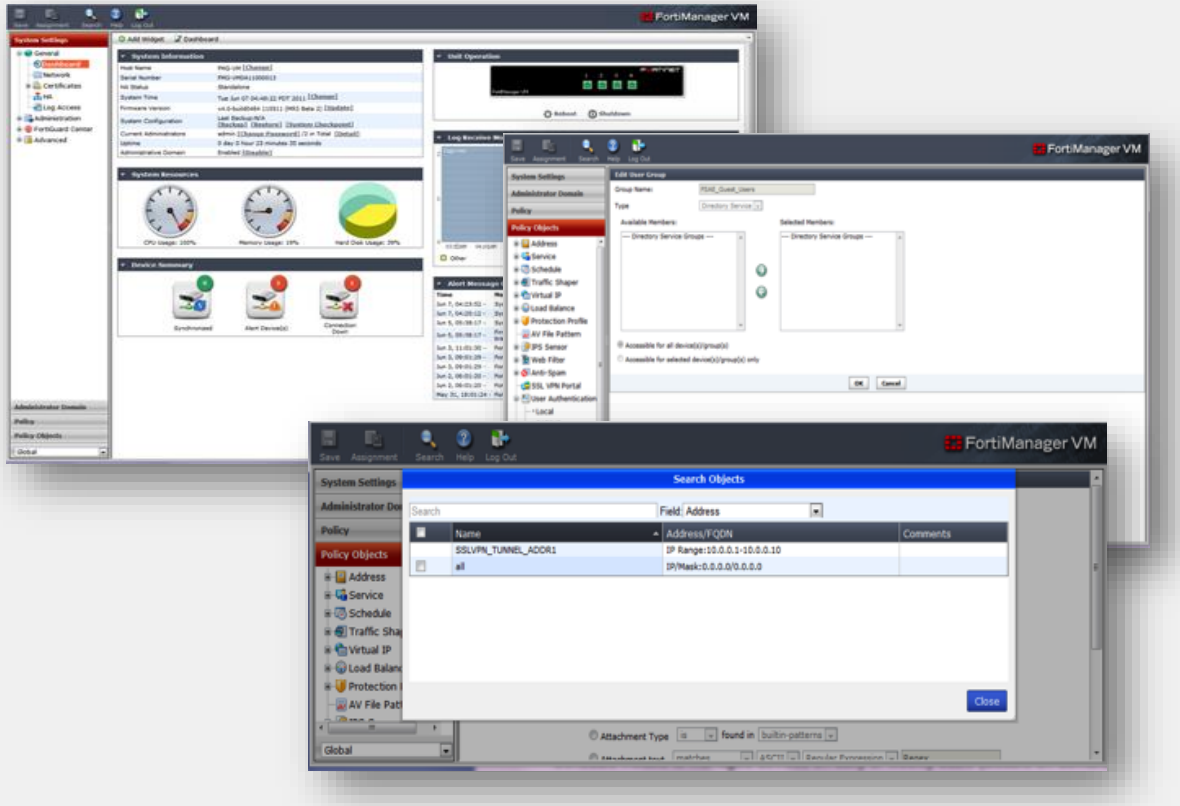
Narzędzie skutecznego zarządzania infrastrukturą bezpieczeństwa Fortinet nawet do tysięcy urządzeń

Domeny administracyjne (ADOMs)
- Pozwala głównemu administratorowi tworzyć wirtualne domeny zarządzania dla innych administratorów

Hierarchiczny system polityk i obiektów
- Globalne obiekty i polityki
- Przypisanie do domen i grup
- Tworzenie wzorców konfiguracji do szybkiego wdrażania

Lokalne przechowywanie danych
- Pozwala na zarządzanie aktualizacjami oprogramowania i baz danych
- Lokalna kopia baz AV, IPS, URL, A/S

Web Portal SDK
- JSON-based API umożliwia tworzenie (sub)portali zarządzania



FortiAnalyzer

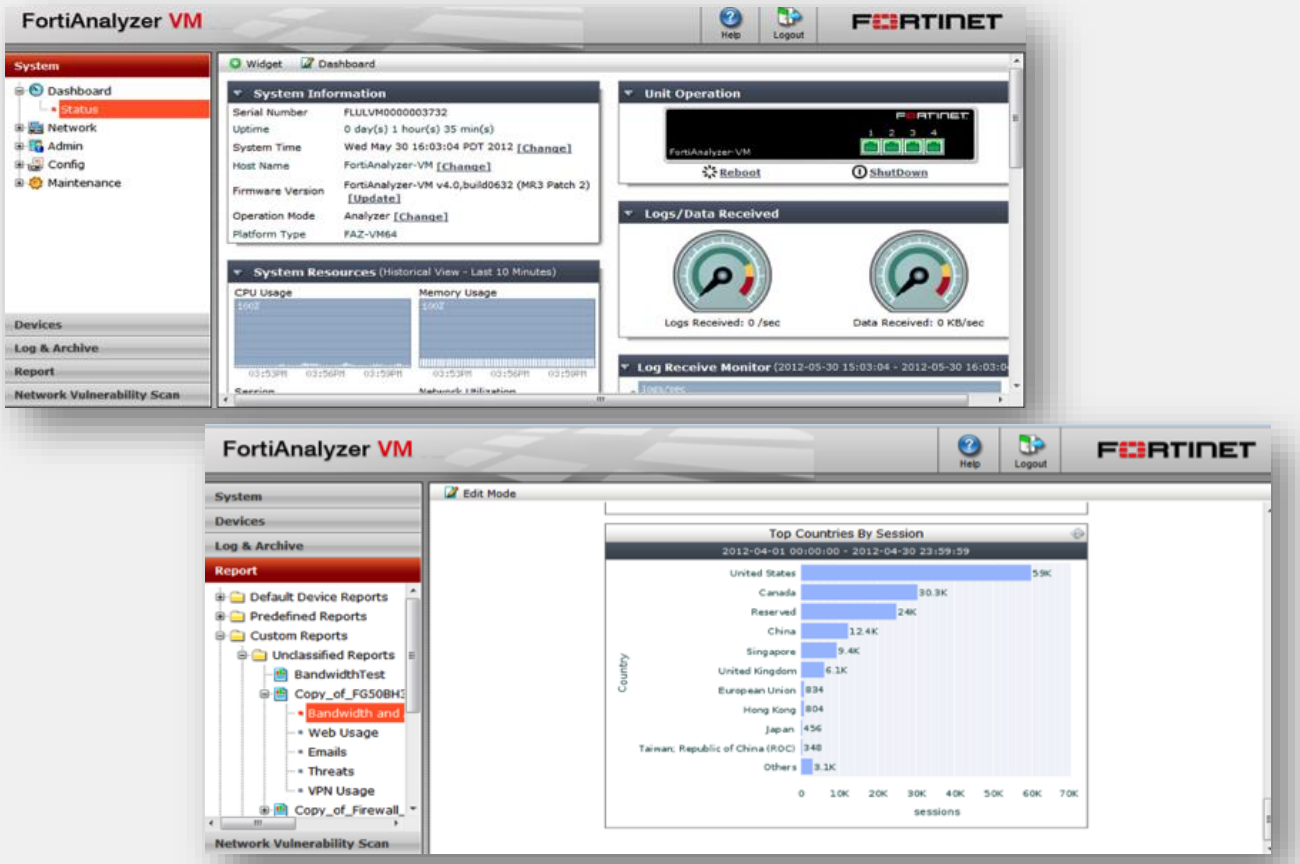
Logowanie, analiza i raporty dla urządzeń marki Fortinet

Zintegrowana rejestracja zdarzeń
- Pojedynczy widok wszystkich urządzeń
- Wbudowana archiwizacja
- Kwarantanna plików

Centralne raportowanie
- Predefiniowane wzorce raportów
- Setki konfigurowalnych tabel i wykresów

Analiza i korelacja
- Ocena podatności
- Analiza i korelacja logów i ruchu sieciowego

Skalowalność
- Wersje HW i wirtualne
- Tryb pracy Collector/Analyzer dla dużych środowisk
- Obsługa dużej ilości zdarzeń na sekundę
- Elastyczność obsługi bazy danych



FortiMail

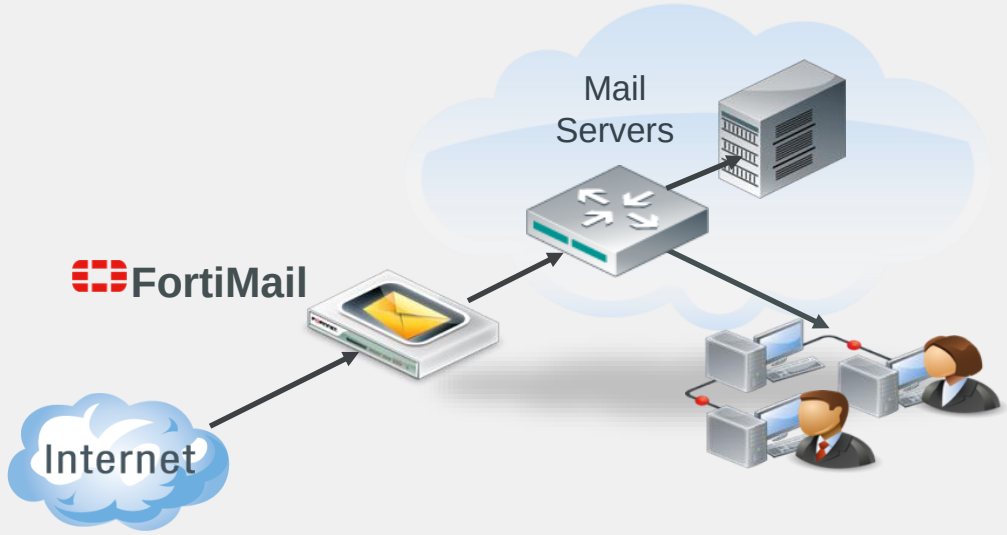
Zaawansowane zabezpieczenie systemów pocztowych, chroniące przez SPAMem, wirusami, phishingiem i malwarem z możliwością kwarantanny i archiwizacji

Specjalistyczny system ochrony poczty
- Zaawansowany system dwukierunkowego filtrowania zapobiega rozprzestrzenianiu SPAMu, wirusów, phishing'u, robaków i innego szkodliwego oprogramowania.

Elastyczne wdrożenie
- Transparent, Gateway, Server

Szyfrowanie
- Ochrona komunikacji krytycznej

Archiwizacja
- Archiwizacja On-box tam, gdzie jest to wymagane biznesowo lub prawnie



Enterprise ATP Bundle

Base Bundle

Antispam

- Ocena nadawcy
- Ocena osadzonych URLi
- Analiza zawartości pod kątem SPAMu i phishingu
- Oddzielne identyfikatory typu “newsletter”

Antivirus

- Sygnatury
- Heurystyka
- Emulation
- Rozpakowywanie i dekrypcja
- Opatentowany Content Pattern Recognition Language (CPRL)

Outbreak Prevention

- Inteligencja przed-sygnaturowa
- Obejmuje rosnące kampanie mailowe i szkodliwe
- Korzysta z mechanizmów threat intelligence

FortiSandbox Cloud

- FortiSandbox utrzymywany przez Fortinet
- Analiza szybka i pełna
- Model subskrypcyjny
- Nie wymaga zakupu i instalacji

Content Disarm and Reconstruction

- Usuwa niebezpieczną aktywną zawartość
- Microsoft Office i Adobe
- Granularne stosowanie
- Przywracanie oryginalnych dokumentów

Click Protect

- Dynamiczna reputacja
- Ocena w chwili „kliknięcia” łącza
- Identyfikacja ostatnio stworzonych / naruszonych stron i nowych kampanii

Impersonation Analysis

- Identyfikacja sfałszowanych maili
- Dynamiczna ochrona powszechnych adresów
- Uzupełnia uwierzytelnianie nadawcy

Elastyczność i skalowalność

Urządzenia

- Wiele modeli
- Obsługa od 2700 do 1.5 miliona wiadomości na godzinę

Oprogramowanie

- Wiele modeli VM
- Elastyczne mechanizmy doboru
- Licencje wieczyste

SaaS

- Tryb Gateway albo Server
- Standard / Premium
- Cena/użytkownik/rok

FortiEMS i FortiClient

Kompleksowa ochrona

FortiEMS, znany również jako Fortinet Endpoint Management System, system centralnego zarządzania zabezpieczeniami końcowymi (endpoint security management). Zapewnienia widoczność i kontrolę nad zabezpieczeniami urządzeń końcowych.

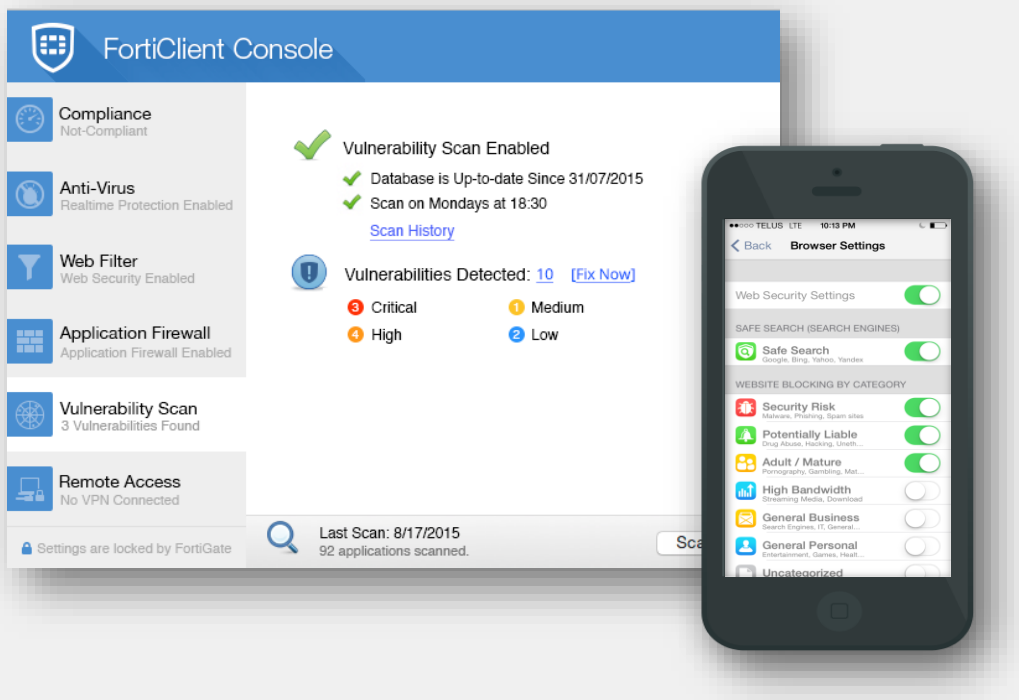
Wielofunkcyjna ochrona

- Elastyczne wdrożenie
- Zintegrowane funkcje bezpieczeństwa

Kontrola urządzeń końcowych

- Wymuszenie zasad zgodności i stosowanie polityk bezpieczeństwa

Centralne logowanie i raportowanie



FortiAuthenticator

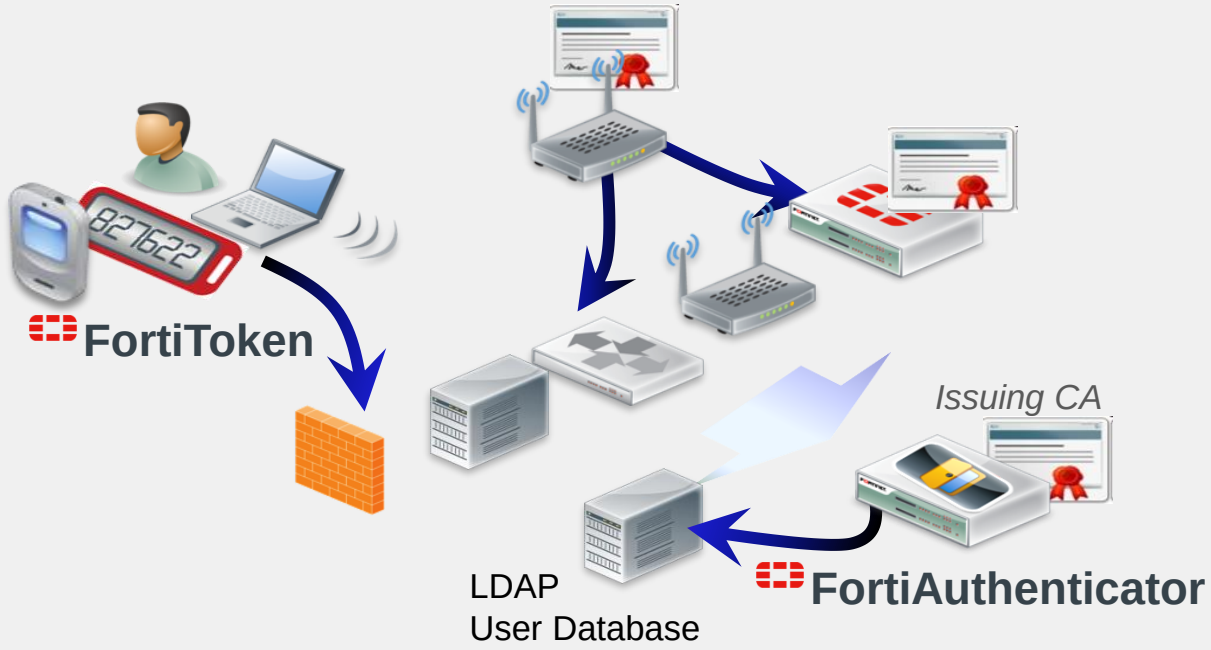
Zarządzanie tożsamością, User Access Control i uwierzytelnianie MFA

Uwierzytelnianie i autoryzacja
- RADIUS, LDAP, 802.1X

Uwierzytelnianie wieloskładnikowe
- FortiToken
- SMS / email

Zarządzanie certyfikatami
- X.509 Certificate Signing, Certificate Revocation
- Remote Device / Unattended Authentication

Fortinet Single Sign-on
- Active Directory Polling
- RADIUS



FortiToken

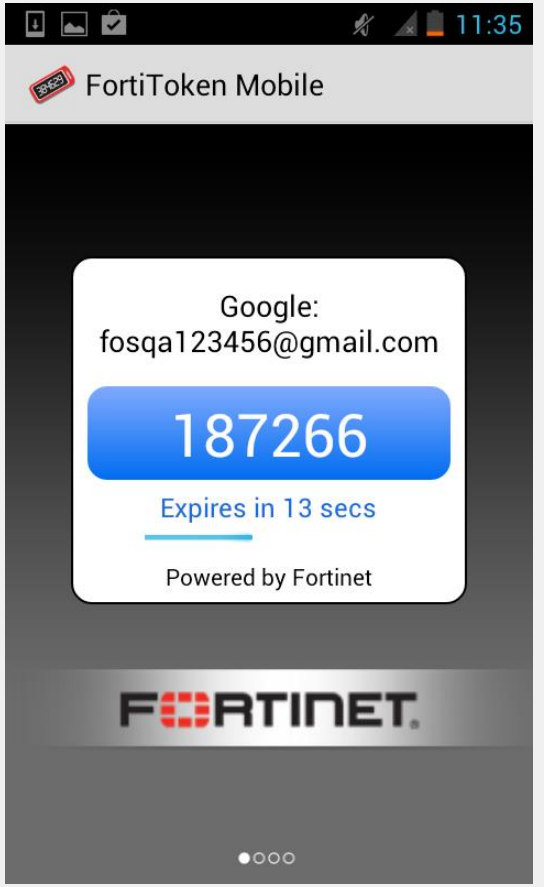
Synchronizowany czasowo Token

Wsparcie dla zaawansowanego uwierzytelnienia

- IPSEC VPN
- SSL VPN
- Login dla administratora
- Captive Web Portal
- Uwierzytelnienie 802.1x
- Web Application Access
- SSO (Single SignOn)

Platformy Uwierzytelnienia

- FortiGate (FOS4.3 and later)
- FortiAuthenticator (FAC 1.4 and later)



FortiSIEM

Korelacja zdarzeń, analiza naruszeń i zarządzanie ryzykiem

- **FortiSIEM to rozwiązanie Security Information and Event Management (SIEM)** jest platformą do zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem, która agreguje i analizuje dane z różnych źródeł w celu monitorowania, oceny i zabezpieczania infrastruktury IT przed zagrożeniami cybernetycznymi.

FortiSIEM

Korelacja zdarzeń, analiza naruszeń i zarządzanie ryzykiem

Centralne monitorowanie bezpieczeństwa FortiSIEM zapewnia jedno, centralne miejsce do monitorowania wszystkich zdarzeń związanych z bezpieczeństwem w całej infrastrukturze IT.

- **Korelacja zdarzeń**
- **Analiza zachowań użytkowników i urządzeń (UEBA)**
- **Zarządzanie konfiguracją i aktywami**
- **Wizualizacja danych**
- **Zautomatyzowane odpowiedzi**
- **Wsparcie dla wielu typów urządzeń**
- **Szybka identyfikacja zagrożeń**
- **Zgodność z regulacjami**

FortiSwitch

Przełączniki Multi Gigabitowe

- Wysoka wydajność i skalowalnoś bezpieczeństwa dla organizacji o zróżnicowanych potrzebach operacyjnych.

Główne korzyści:

- ✓ Wysoka gęstość portów
- ✓ Zintegrowane zasilanie przez Ethernet
- ✓ Łączy punkty dostępu, urządzenia peryferyjne, kamery, telefony
- ✓ Tworzy zintegrowaną, bezpieczną sieć

FortiAP 431/433F

Indoor | 802.11ax | Potrójne Radio | 4x4

1. 1 x 2.5GE RJ45 Interfejs
2. 1 x GE RJ45 Interfejs
3. 1x RS-232 RJ45 Port Szeregowy

a/b/g/n /ac/ax

1. 1 x 2.5GE RJ45 Interfejs
2. 1 x GE RJ45 Interfejs
3. 1x RS-232 RJ45 Port Szeregowy

a/b/g/n /ac/ax

	FAP-431F	FAP-433F
Środowisko pracy	Wysoka gęstość, wysoka wydajność indoor	Wysoka gęstość, wysoka wydajność indoor
Liczba Anten	5 Internal + 1 BLE Internal	5 External (RP-SMA) + 1 BLE indoor
Rx / Tx	4x4	4x4
Radio 1	2.4 GHz b/g/n/ax (1,147 Mbps)	2.4 GHz b/g/n/ax (1,147 Mbps)
Radio 2	5GHz a/b/g/n/ac/ax (2,402 Mbps)	5GHz a/b/g/n/ac/ax (2,402 Mbps)
Radio 3	2.4/5.0 GHz (tylko skaner)	2.4/5.0 GHz (tylko skaner)
PoE	802.3at	802.3at

Fortinet jest rozpoznawanym liderem według Analityków

Dla rozwiązań Firewall i SD-WAN

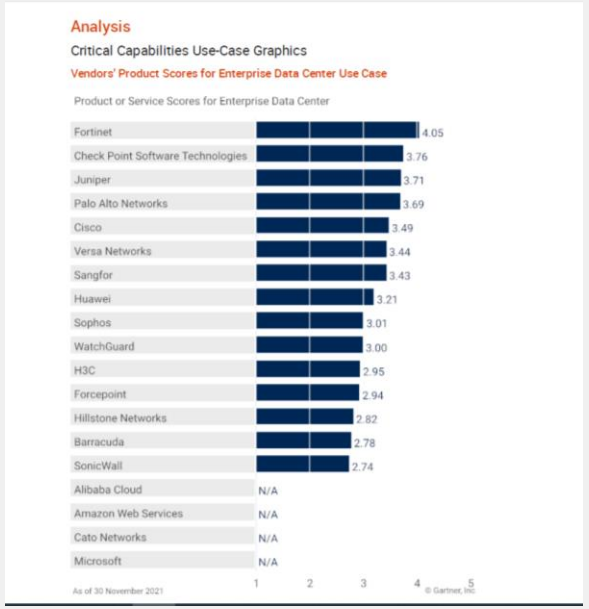
11/2021 Magic Quadrant™ dla Firewalli Sieciowych

Fortinet rozpoznawany jako Leader rynku firewalli od 2021 w Magicznym Kwadrancie Gartnera

09/2022 Magic Quadrant™ dla rozwiązań SD-WAN

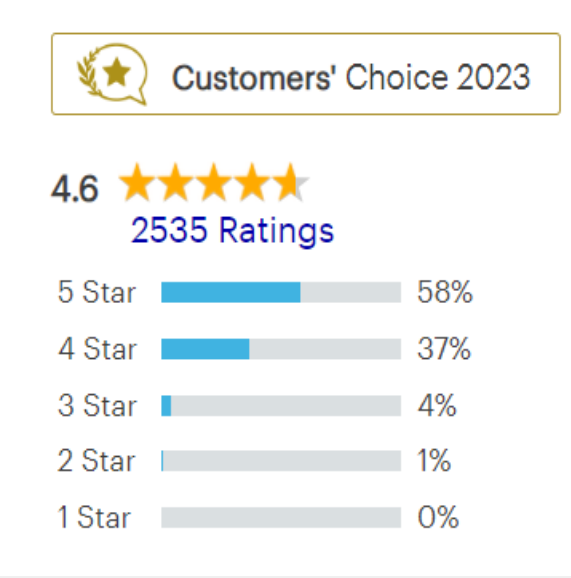
Fortinet najlepiej spozycjonowany dostawca od dwóch lat z rzędu dla rozwiązań SD-WAN

01/2022 Konieczna Funkcjonalność dla Firewalli



Fortinet #1 w zastosowaniach w przedsiębiorstwach i centrach danych

03/2023 Gartner Customer choice



Fortinet najlepszym dostawcą według klientów badanych przez Gartner


FORTINET