



Bezpieczna praca w erze cyfrowych zagrożeń

Grzegorz Gondek, Business Development Manager
Szymon Poliński, Systems Engineer Manager

Zimowa Akademia Fortinet



3 Sesje:

Dlaczego klasyczne DLP nie działa?
Nowoczesne podejście do ochrony danych
i ryzyka wycieku informacji

Bezpieczna praca w erze cyfrowych zagrożeń

Od pułapki do wykrycia, czyli detekcja
i neutralizowanie adversarzy w naszej sieci
26 lutego 2026, godz. 11:00 – 12:30

Secure Access Service Edge

Najlepsze rozwiązanie do ochrony pracowników hybrydowych



SWG
Secure Internet Access



FWaaS
Secure Internet Access



CASB, DLP
Secure SaaS Access



DEM
Digital Experience



SB
Secure Browser



Clientless ZTNA
Sharing internal resources



SD-WAN
Connectivity, Private Access

#1 Broni przed zagrożeniami z Internetu

#2 Bezpiecznie łączy z zasobami on-prem / cloud

#3 Upraszcza utrzymanie i zarządzanie środowiskiem



SASE - Najlepsze rozwiązanie do ochrony pracowników hybrydowych



SWG
Secure Internet Access



FWaaS
Secure Internet Access



CASB, DLP
Secure SaaS Access



DEM
Digital Experience



SB
Secure Browser



Clientless ZTNA
Sharing internal resources



SD-WAN
Connectivity, Private Access

#1 Broni przed zagrożeniami z Internetu

#2 Bezpiecznie łączy z zasobami on-prem / cloud

#3 Upraszcza utrzymanie i zarządzanie środowiskiem

Pytanie do publiczności

Czy masz już doświadczenia z usługami Secure Access Service Edge?



Parę słów o zagrożeniach z Internetu



Fortinet Global Threat Landscape Report 2025

Skala zagrożeń w liczbach



 **36 000**

skanów / sekunde

+16.7% r/r

 **97 mld**

prób eksploatacji

w ciągu 2025 r.

 **500%**

wzrost infostealerów

Redline, Vidar

 **1.7 mld**

skradzionych poświadczeń

na forach darknet

 **42%**

wzrost kradzieży poświadczeń

100+ mld rekordów

 **5.4 dnia**

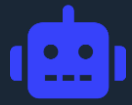
czas do eksploatacji

od ujawnienia CVE



Fortinet Global Threat Landscape Report 2025

AI-Powered Cybercrime & CAAS



Narzędzia AI używane przez atakujących



FraudGPT

Generowanie phishingu i malware bez restrykcji etycznych



BlackmailerV3

Automatyczne tworzenie kampanii extortion



ElevenLabs

Klonowanie głosu dla vishing (voice phishing)



Voicemy.ai

Deepfake głosu do social engineering



LLM-powered CaaS

Automatyzacja ofert Cybercrime-as-a-Service



Darknet & CaaS Marketplace

Oferty Initial Access Brokers



■ Corporate Credentials (20%) ■ RDP Access (19%) ■ Admin Panels (13%)
■ Web Shells (12%) ■ Inne (36%)

+40 000 nowych CVE w NVD (+39% r/r) | 331 zero-day na darknet



ENISA THREAT LANDSCAPE 2025

Dane: lipiec 2024 — czerwiec 2025 | ~4 900 incydentów przeanalizowanych

~4 900

incydentów w UE

przeanalizowanych przez ENISA

38%

cel: administracja publiczna

hacktyvisci + nation-state

18.2%

ataki na OT / przemysł

wzrost ataków na infrastrukturę

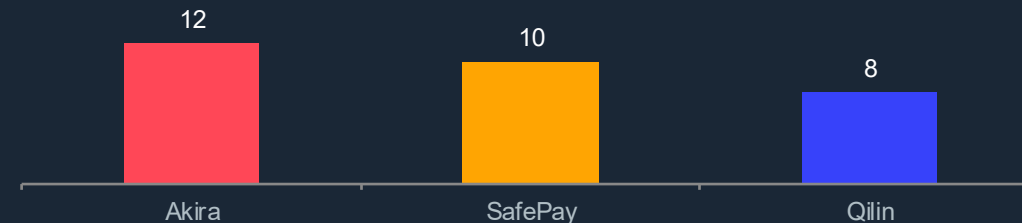
80%

incydentów = hacktywizm

głównie DDoS (2% skutecznych)

Top Ransomware w UE

82 warianty ransomware użyte przeciwko organizacjom w UE



Polska, Czechy, Rumunia

Kraje wspierające Ukrainę pod szczególną obserwacją grup APT (ENISA 2025)

Data breaches: infrastr. cyfrowa 27.7%, admin. publ. 17%

Ransomware claims: manufacturing 14.9% w UE



POLSKA — CERT POLSKA / CSIRT NASK 2024-2025

Raport roczny CERT Polska za 2024 + dane bieżące 2025

236 tys.

incydentów w 2025

2x wzrost vs 2024 (111 tys.)

620 tys.

zgłoszeń w 2025

vs 600 tys. w 2024

~300

incydentów dziennie (2024)

+29% r/r, +62% zgłoszeń

176

ataków ransomware (2025)

vs 140 w 2024 (+26%)



97% incydentów = oszustwa

Phishing, faking stron bankowych
i serwisów społecznościowych,
fałszywe ogłoszenia (OLX, Allegro)



160 tys. szkodliwych domen

Zablokowanych na Liście Ostrzeżeń
CERT Polska (sty-wrz 2025).
AI wspiera przestępców w wykrywaniu
podatności.



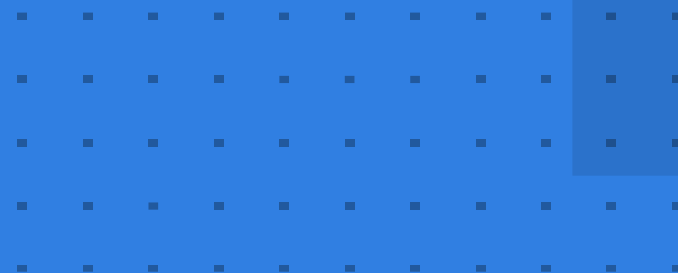
Atak na sektor energii (XII.2025)

Destrukcyjny atak na farmy wiatrowe,
fotowoltaikę i elektrociepłownie.
CERT PL opublikował raport z incydentu.



Pytanie do publiczności

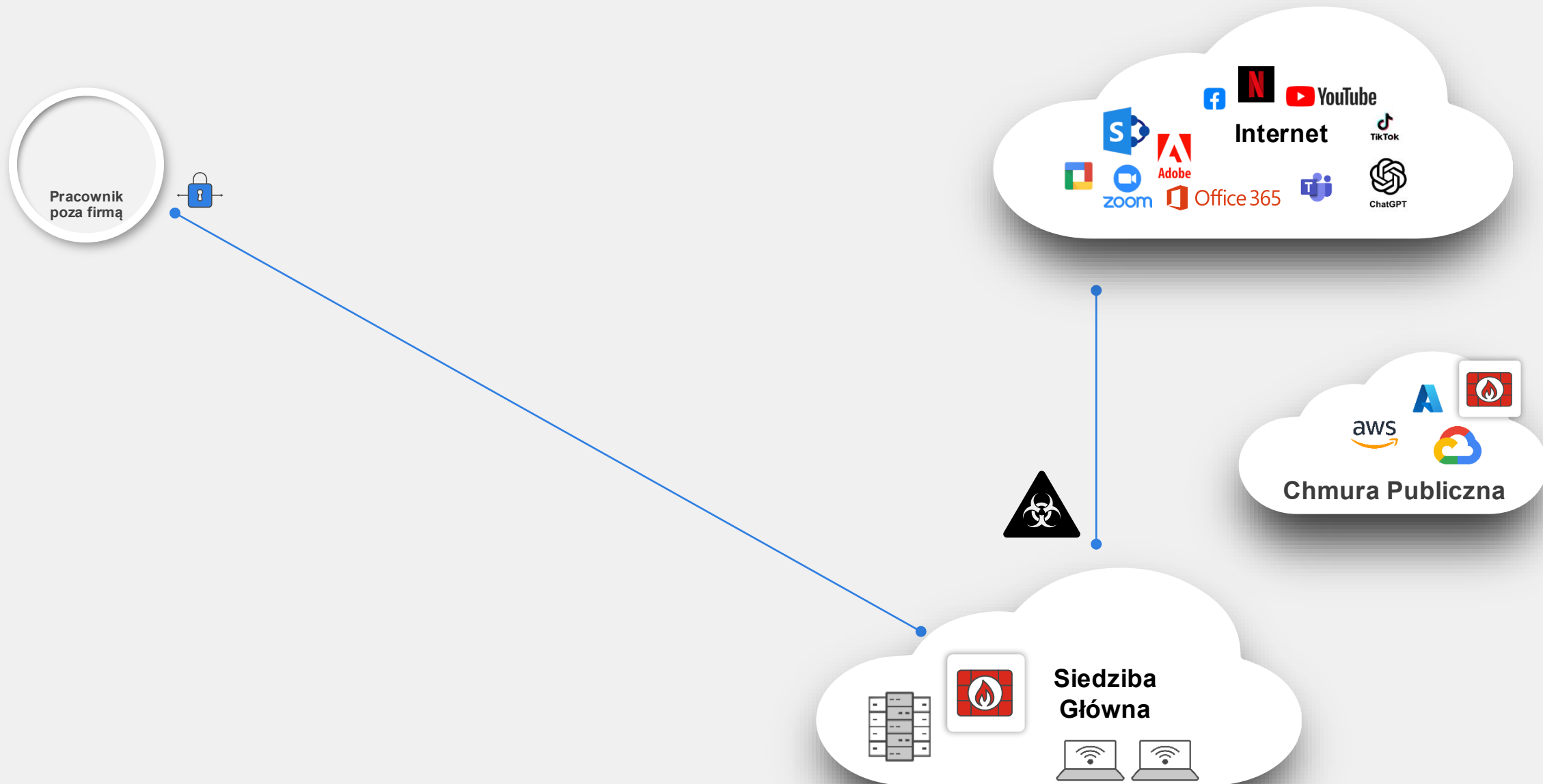
Które z wymienionych zagrożeń uważają Państwo za najważniejsze?



Dotychczasowe podejście do ochrony

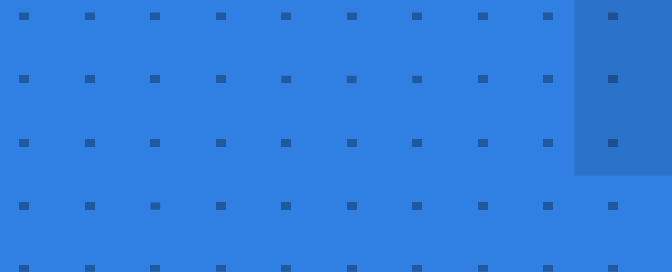


Podjęcie do ochrony użytkowników



Pytanie do publiczności

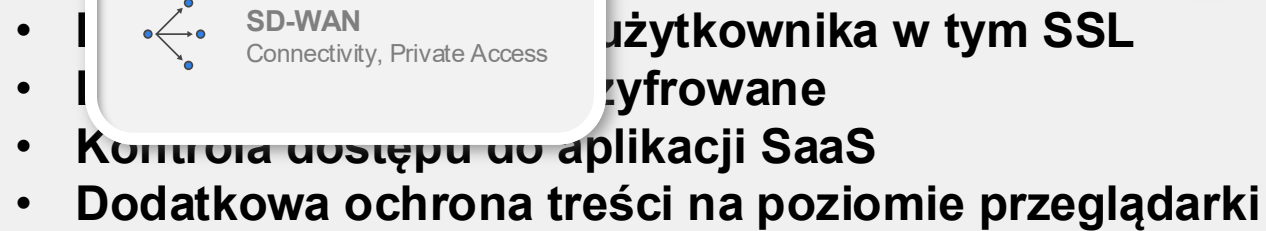
Z jakimi największymi problemami spotykają się Państwo obecnie w organizacji bezpiecznego dostępu do danych?



#1

Ochrona przed zagrożeniami z Internetu





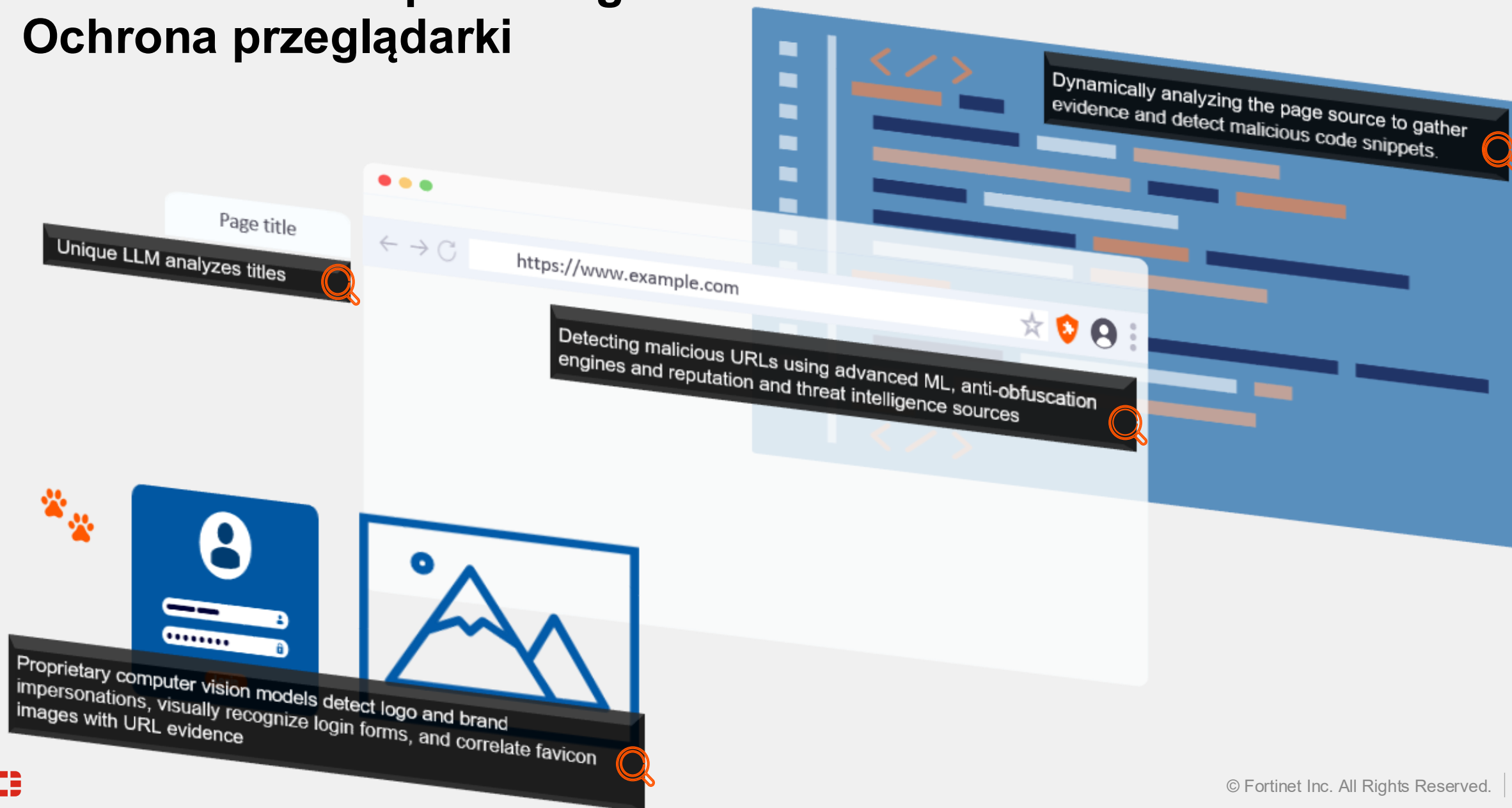
SASE - Ochrona przed zagrożeniami z Internetu

Ochrona przeglądarki



SASE - Ochrona przed zagrożeniami z Internetu

Ochrona przeglądarki



SASE - najlepsze rozwiązanie do ochrony pracowników hybrydowych



SWG
Secure Internet Access



FWaaS
Secure Internet Access



CASB, DLP
Secure SaaS Access



DEM
Digital Experience



SB
Secure Browser



Clientless ZTNA
Sharing internal resources



SD-WAN
Connectivity, Private Access

#1 Broni przed zagrożeniami z Internetu

#2 Bezpiecznie łączy z zasobami on-prem / cloud

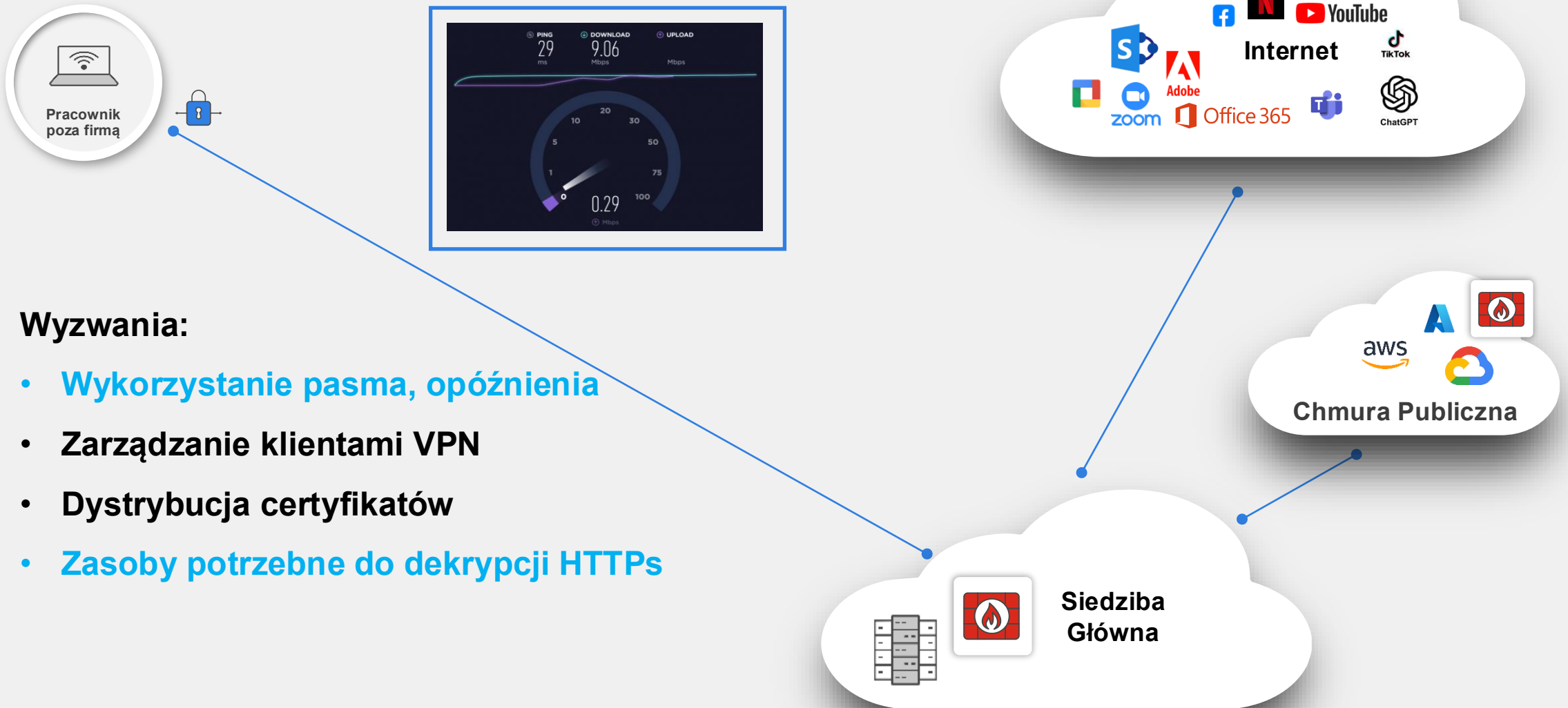
#3 Upraszcza utrzymanie i zarządzanie środowiskiem

Pytanie do publiczności

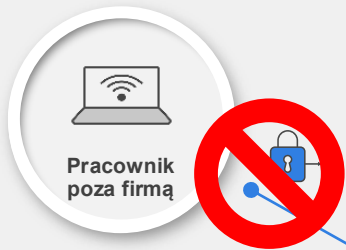
Jakie narzędzia lub metody realizujące dostęp do danych są dziś wykorzystywane?



Dostęp zdalny - Remote Access VPN

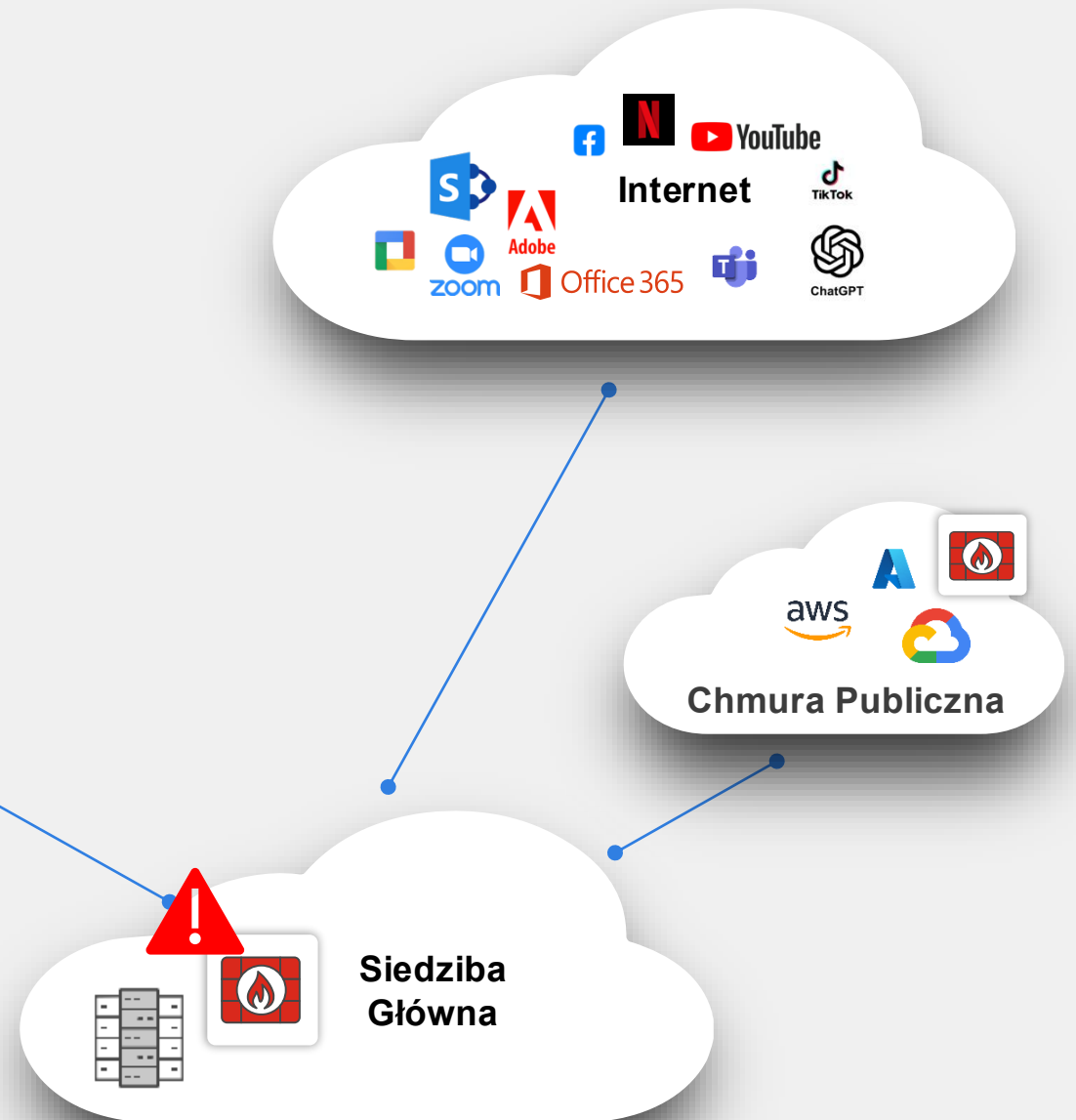


Dostęp zdalny - Always-On VPN

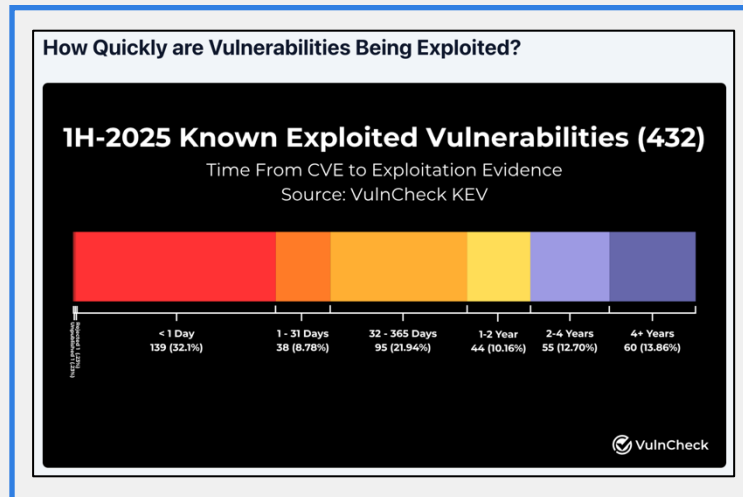
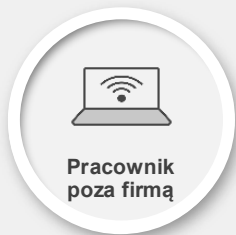


Wyzwania:

- Wykorzystanie pasma, opóźnienia
- Zarządzanie klientami VPN
- Dystrybucja certyfikatów
- Zasoby potrzebne do dekrypcji HTTPs
- **Dostępność usługi Always-On VPN**



Dostęp zdalny - Always-On VPN



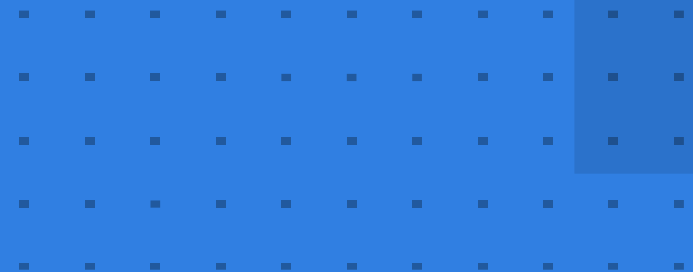
Wyzwania:

- Wykorzystanie pasma, opóźnienia
- Zarządzanie klientami VPN
- Dystrybucja certyfikatów
- Zasoby potrzebne do dekrypcji HTTPs
- Dostępność usługi Always-On VPN
- Aktualizacje, Utrzymanie
- DDoS, Ataki na usługę



Bezpieczny dostęp do
zasobów wewnętrznych

#2



SASE - Bezpieczny dostęp do zasobów wewnętrznych



Zastępuje VPN

- Automatyczne łączenie, posture check, ZTNA
- Wysoka dostępność – HA na poziomie usługi
- Technologia SDWAN optymalizuje połączenia
- Kieruje do DC tylko wewnętrzny ruch, już przefiltrowany
- Dodatkowo możliwe bezpośrednie połączenia

SASE - najlepsze rozwiązanie do ochrony pracowników hybrydowych



SWG
Secure Internet Access



FWaaS
Secure Internet Access



CASB, DLP
Secure SaaS Access



DEM
Digital Experience



SB
Secure Browser



Clientless ZTNA
Sharing internal resources



SD-WAN
Connectivity, Private Access

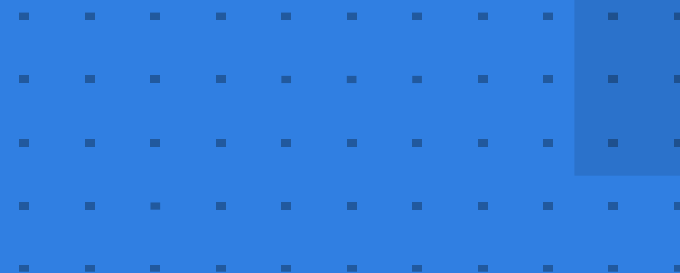
#1 Broni przed zagrożeniami z Internetu

#2 Bezpiecznie łączy z zasobami on-prem / cloud

#3 Upraszcza utrzymanie i zarządzanie środowiskiem

Uprozczone utrzymanie oraz zarządzanie środowiskiem

#3

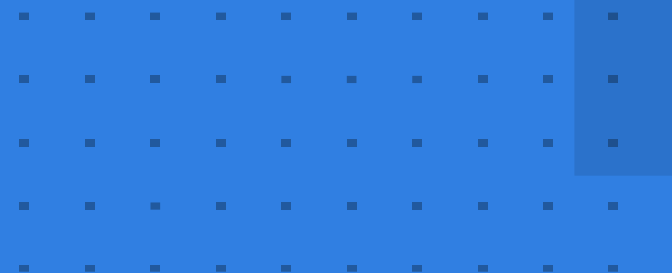


Utrzymanie, aktualizacje, skalowanie – to wszystko ważny koszt

Obszar / Czynność	SaaS (automatyczne)	On-Prem (Praca Admina)	Co leży w gestii Administratora?
Backup przed aktualizacją	Automatyczny	Ręczny	Snapshoty VM, backup DB, config export
Testowanie na staging	Dostawca testuje	Ty testujesz	Środowisko staging lustrzane do PROD
Rollback w razie awarii	Automatyczny	Ręczny plan	Procedura rollback + przetestowany RTO
Kompatybilność zależności	Gwarantowana	Ty sprawdzasz	Wersje OS, biblioteki, API, integracje
Aktualizacja certyfikatów	Auto-renewal	Ręczna wymiana	Śledzenie dat wygaśnięcia, łańcuch CA
Patching OS / firmware	Dostawca	Ty robisz	Okno serwisowe, testy, reboot
Hardening konfiguracji	Domyślny	Twój hardening	CIS Benchmarks, polityki GPO, FW rules
Monitoring po aktualizacji	Wbudowany	Twój stack	Zabbix/Grafana/SIEM – alerty, dashboardy
Skan podatności	Ciągły	Ty skanujesz	Nessus/Qualys po każdej zmianie
Dokumentacja zmian	Changelog dostawcy	Ty dokumentujesz	CMDB, wiki, diagramy, raporty
Compliance / audyt	Certyfikaty dostawcy	Twoja odpowiedzialność	PCI-DSS, ISO 27001, NIS2 – dowody
Komunikacja z użytkownikami	Częściowa	Ty komunikujesz	Okno serwisowe, e-mail, status page
HA / failover podczas update	Zero downtime	Ty planujesz	Failover, drain, load balancer
Aktualizacja agentów (AV/EDR)	Push z konsoli	Zależy od konfiguracji	Sprawdź kompatybilność z nową wersją



Pytanie do publiczności



Które z wyzwań dotyczących utrzymania i zarządzania dotyczą Państwa środowiska?



SASE - Utrzymanie i zarządzanie środowiskiem



- Jedna polityka bezpieczeństwa
- Zintegrowane komponenty, pełny stos
- Automatyczne aktualizacje, utrzymanie środowiska
- Skalowanie wg potrzeb, jedna licencja

SASE - Zunifikowane zarządzanie



SWG
Secure Internet Access



FWaaS
Secure Internet Access



CASB, DLP
Secure SaaS Access



DEM
Digital Experience



SB
Secure Browser



Clientless ZTNA
Sharing internal resources



SD-WAN
Connectivity, Private Access

Korzyści z Unified SASE

Integracja, konsolidacja, kompleksowa widoczność

Uproszczenie infrastruktury

Zmniejszona liczba dostawców rozwiązań wymagających integracji

Uprozczone operacje oraz redukcja kosztów

Konsolidacja i integracja

Ścisła integracja między sieciami a bezpieczeństwem dzięki zunifikowanemu zarządzaniu

Szybsza krzywa uczenia się

Elastyczność

Elastyczne egzekwowanie reguł bezpieczeństwa w pracy lokalnej i w chmurze

Konsekwentna ochrona przed zagrożeniami napędzana przez AI/ML

SASE – Spojrzenie na koszty



FortiSASE - najlepsze rozwiązanie do ochrony pracowników hybrydowych



SWG
Secure Internet Access



FWaaS
Secure Internet Access



CASB, DLP
Secure SaaS Access



DEM
Digital Experience



SB
Secure Browser



Clientless ZTNA
Sharing internal resources



SD-WAN
Connectivity, Private Access

#1 Broni przed zagrożeniami z Internetu

#2 Bezpiecznie łączy z zasobami on-prem / cloud

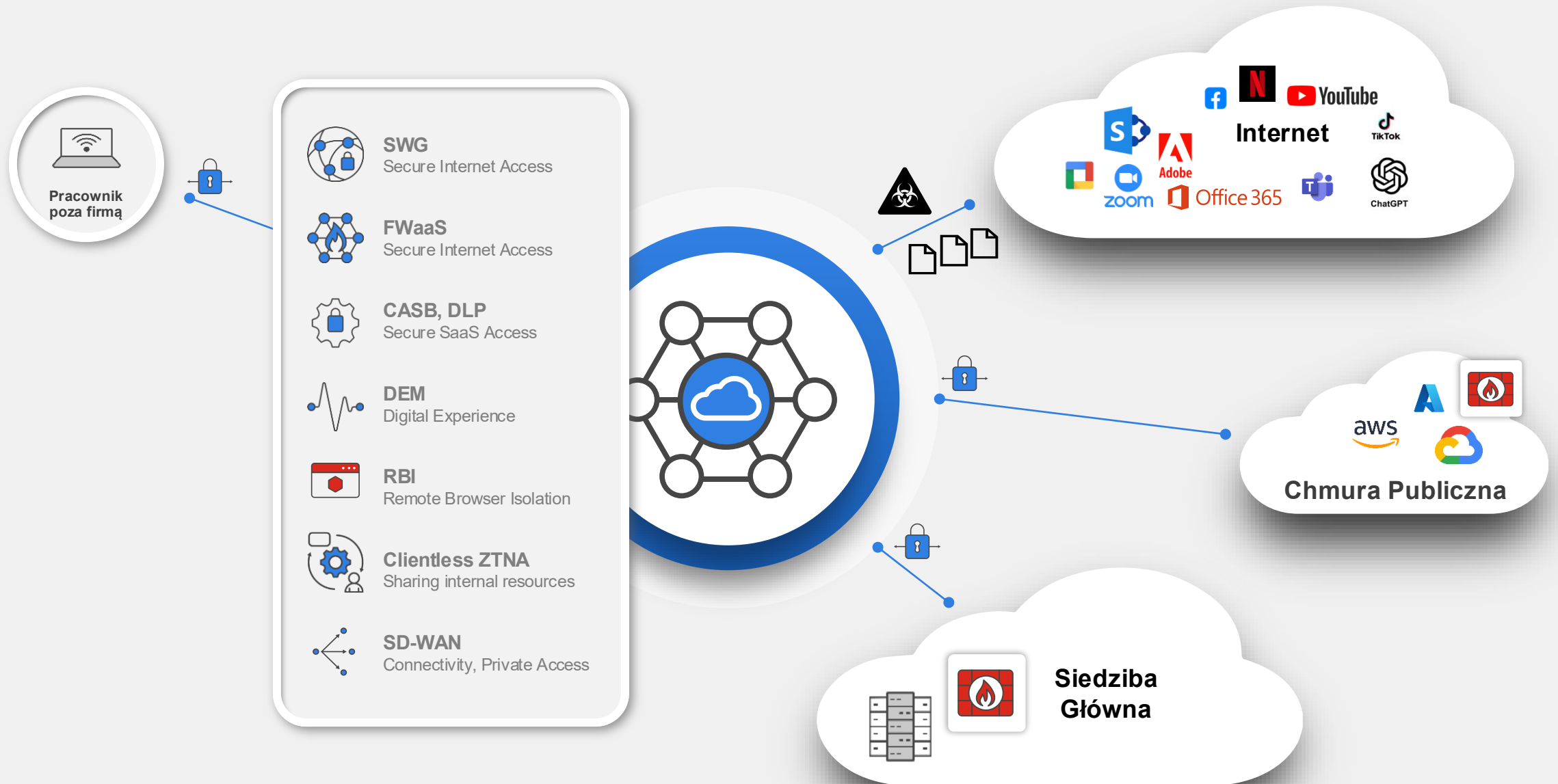
#3 Upraszcza utrzymanie i zarządzanie środowiskiem



FortiSASE



Fortinet Secure Access Service Edge



Fortinet Secure Access Service Edge



Global Coverage
\$1B+ Investment
in Infrastructure



3.3M+ Owned
1.0M+ Leased
4.3M+ Total Sq Ft



Cloud Locations
superior user
experience



FortiStack
Organically built
integrated solutions



Cost Savings
Drive Competitive
Advantage



- Fortinet-owned Security POP
- Fortinet Co-location security POP
- Google Cloud Compute Security POP

2025 Gartner® MQ dla platform SASE - Leader



*Illustrates **Completeness of Vision** and **Ability to Execute***

Pozycja
Fortinet SASE



Gartner

Leader in SD-WAN
Magic Quadrant

Gartner

Leader in Hybrid
Mesh Firewall
Magic Quadrant

Gartner

Leader in Wired
and Wireless LAN
Magic Quadrant

Fortinet
Unified SASE
AAA
Secure Access Service Edge (SASE)
October 29, 2024

YAM CRO
WEB CYBER RISK INSURANCE

Fortinet Secure Access Service Edge

Funkcja	Standard	Advanced	Comprehensive
SWG & FWaaS	●	●	●
FortiClient & EPP	●	●	●
ZTNA	●	●	●
CASB	●	●	●
DLP	●	●	●
Sandbox	●	●	●
DEM		●	●
Integracja SOCaaS		●	●
Endpoint Forensics		●	●
Dedykowane adresy IPs	●	●	●
Wsparcie - On-boarding		●	●
4 POPs	Lokalizacje Fortinet	Lokalizacje Fortinet + Chmury publiczne włączając Polskę	Lokalizacje Fortinet + Chmury publiczne (Premium NW Tier)

Szczegóły

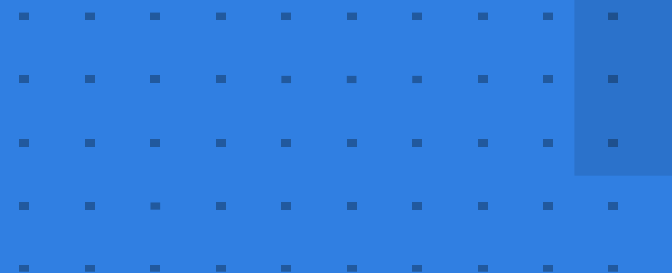
Zawiera 3 urządzenia per użytkownik
Wsparcie FortiCare Premium 24/7
Wymagana dodatkowa licencja SPA dla odpowiedniego modelu urządzenia Fortigate

"Fortinet provides excellent value and it's BOMs are the simplest of any vendor in the SASE market"
(2024 Gartner Single Vendor SASE MQ)

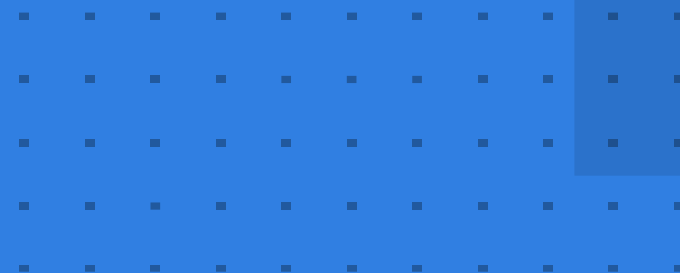


Pytanie do publiczności

Czy byliby Państwo zainteresowani krótką, bezpłatną prezentacją rozwiązania dopasowaną do Państwa potrzeb?



Podsumowanie



FortiSASE - najlepsze rozwiązanie do ochrony pracowników hybrydowych



SWG
Secure Internet Access



FWaaS
Secure Internet Access



CASB, DLP
Secure SaaS Access



DEM
Digital Experience



SB
Secure Browser



Clientless ZTNA
Sharing internal resources



SD-WAN
Connectivity, Private Access

- **Broni przed zagrożeniami z Internetu**
- **Bezpiecznie łączy z zasobami on-prem / cloud**
- **Upraszcza utrzymanie i zarządzanie środowiskiem**