



Praca zdalna. Ochrona i kontrola

Wojciech Ciesielski Major Account Manager, Fortinet

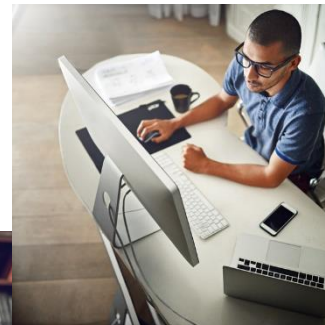
Adam Łobodziński Inżynier Systemowy, Betacom



Ochrona danych – czego uczy nas pandemia
e-konferencja // 3 czerwca 2020r

Możliwość stała się standardem

...praktyka pokazała, że
ograniczenia istniały tylko w
głowach...



Wyzwania środowiska telepracy

- Domowa sieć komputerowa – stabilność łącza, wielość urządzeń
- Zapewnienie bezpieczeństwa komputera
- Ochrona informacji składowanych na urządzeniach
- Bezpieczne przesyłanie danych przez Internet



Urządzenia domowe mogą nieść ryzyko przechwycenia poufnych informacji. Należy stosować regułę „Zero Trust”.

Wyzwania środowiska telepracy

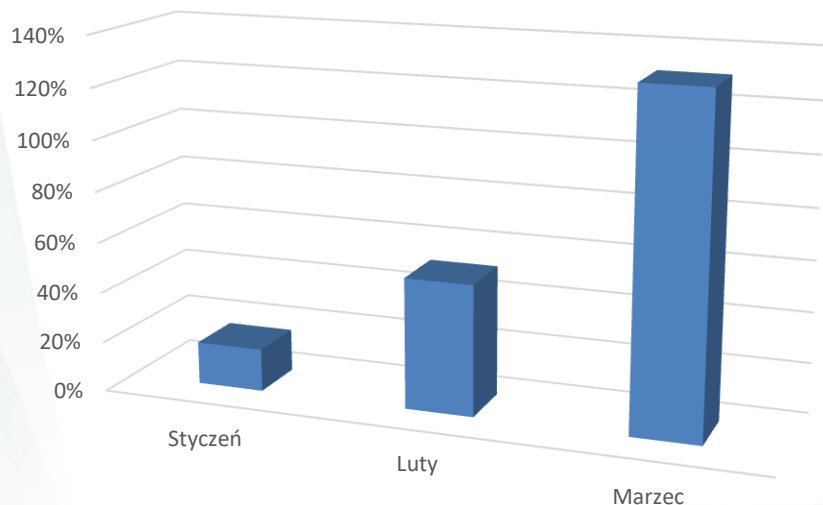
- Sieć komputerowa zaprojektowana pod użytkowników wewnątrz firmy
- Aplikacja SaaS są łatwe do wdrożenia i bardzo niezawodne, obsługują zwiększone obciążenia
- Wersje mobilne aplikacji zwiększają liczbę miejsc, w których znajdują się informacje.



Shadow IT - ryzyko rozprzestrzeniania się poufnych danych w wielu ryzykownych i dostępnych aplikacjach.

Krajobraz zagrożeń dla telepracy

Przyrost r/r wirusów I kw. 2020

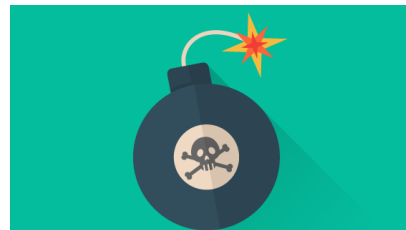


- Niezabezpieczone domowe sieci komputerowe, przypadkowy sprzęt
- Przeorientowanie kierunku działań cyberprzestępców
- Ponad 600 nowych kampanii phishingowych dziennie
- Wzrost liczby wirusów komputerowych

Kluczowe założenia dla telepracy

Sieci i urządzenia zawierają zagrożenia

- Zasada „Zero-Trust” i wieloskładnikowe uwierzytelnianie
- Kontrola dostępu do sieci firmowej (NAC)



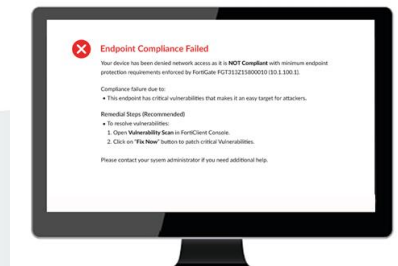
Komunikacja podatna na podsłuchy, przejęcia, modyfikacje

- Szyfrowanie kanałów komunikacji (VPN)
- Ochrona i monitorowanie bram dostępu do sieci firmowej



Urządzenia **BĘDĄ** zainfekowane złośliwym oprogramowaniem

- Zaawansowana ochrona stacji końcowych (EDR)
- Ochrona przed wyciekiem informacji, szyfrowanie
- Kontrola zachowania zgodności i zarządzanie



Fortinet Security Fabric

ROZLEGŁA

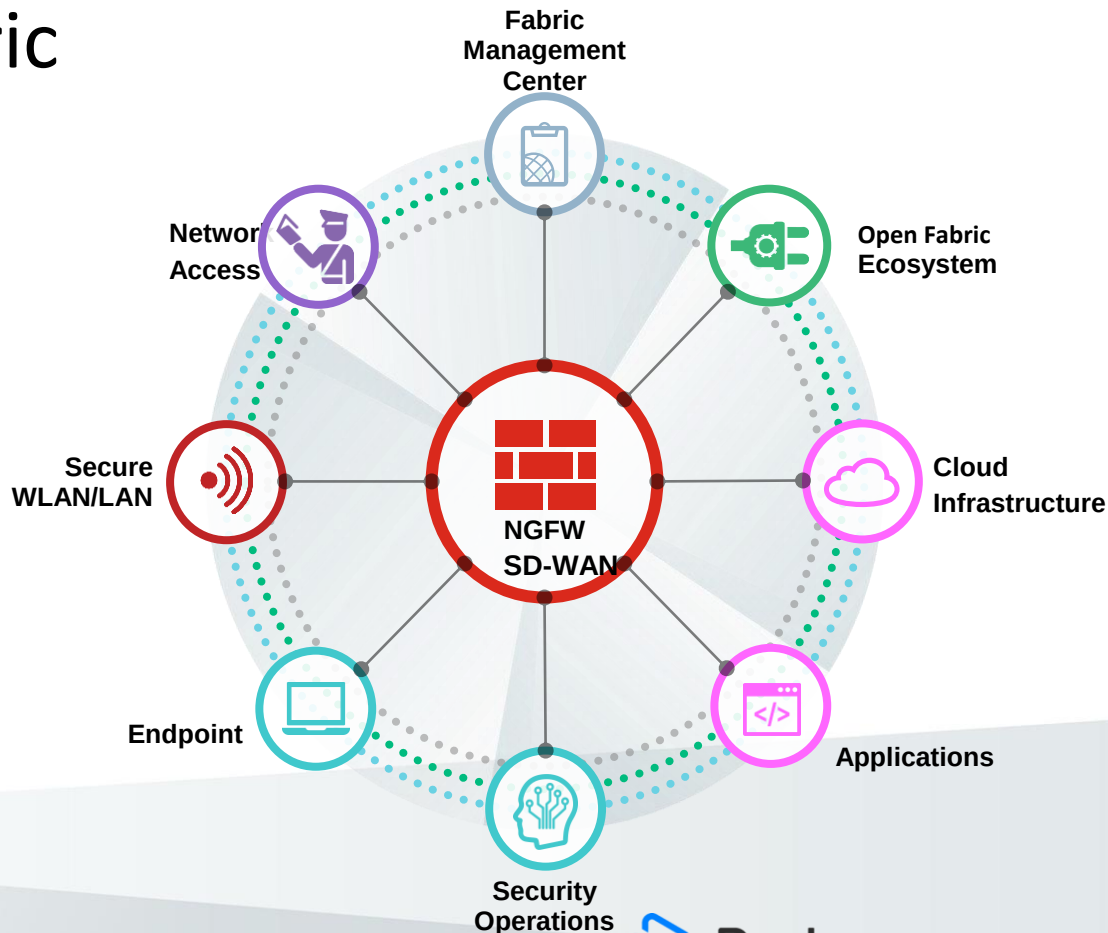
widoczność całej powierzchni ataku

ZINTEGROWANE

rozwiązanie, które zmniejsza złożoność obsługi wielu produktów punktowych

AUTOMATYCZNY

przepływ pracy w celu zwiększenia szybkości operacji i reakcji na zagrożenia



BEZPIECZNA PRACA ZDALNA WEDŁUG FORTINET

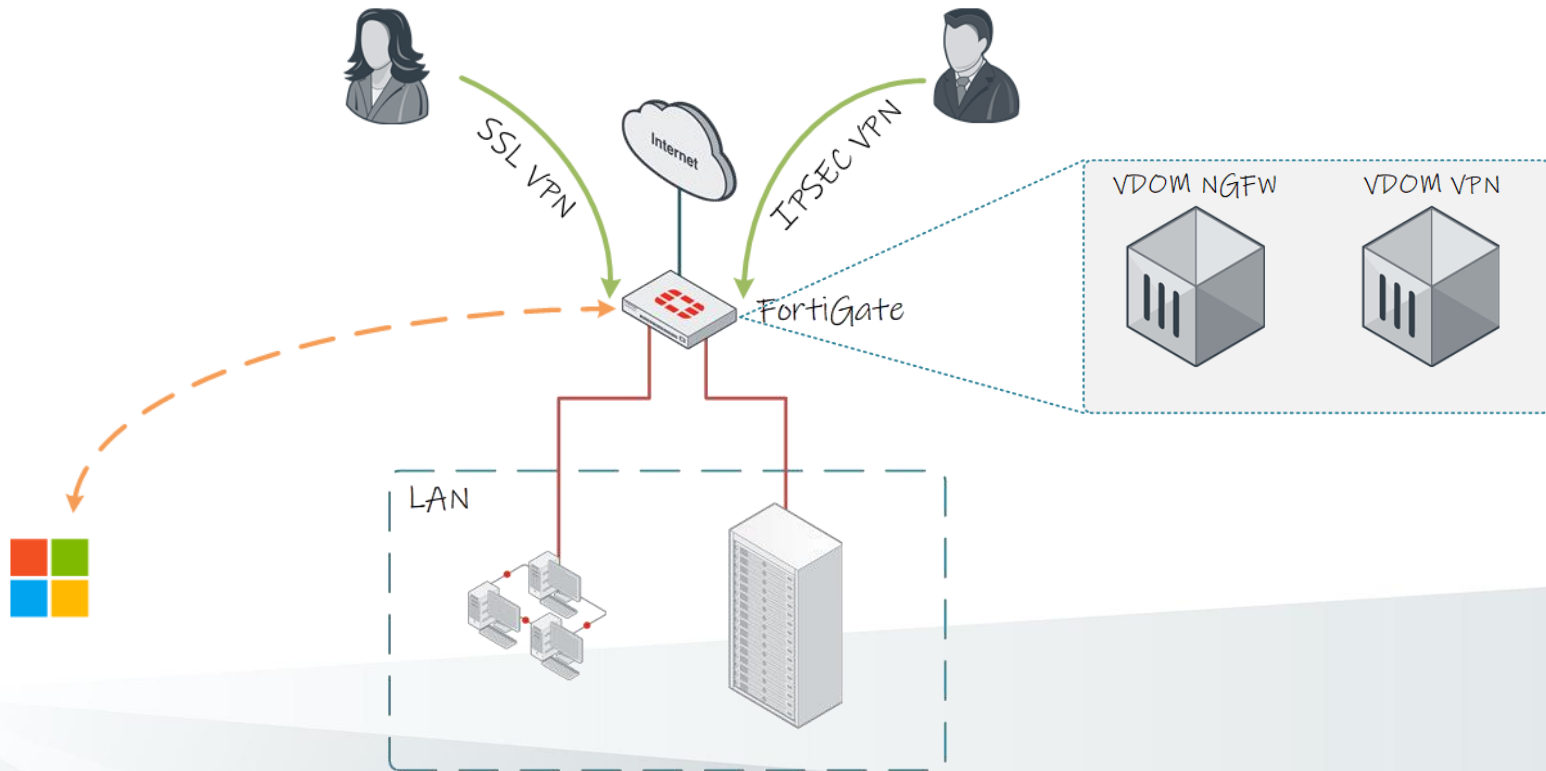
w praktyce

WYKORZYSTAJ CO MASZ

MAM JUŻ FORTIGATE ALE..

- NIE MAM LICENCJI NA VPN
- NIE MAM LICENCJI NA OPROGRAMOWANIE DOSTĘPOWE
- WYKORZYSTUJĘ GO DO CZEGO INNEGO
- ZDALNYM DOSTĘPEM ZAJMUJE SIĘ INNY ZESPÓŁ

WYKORZYSTAJ CO MASZ

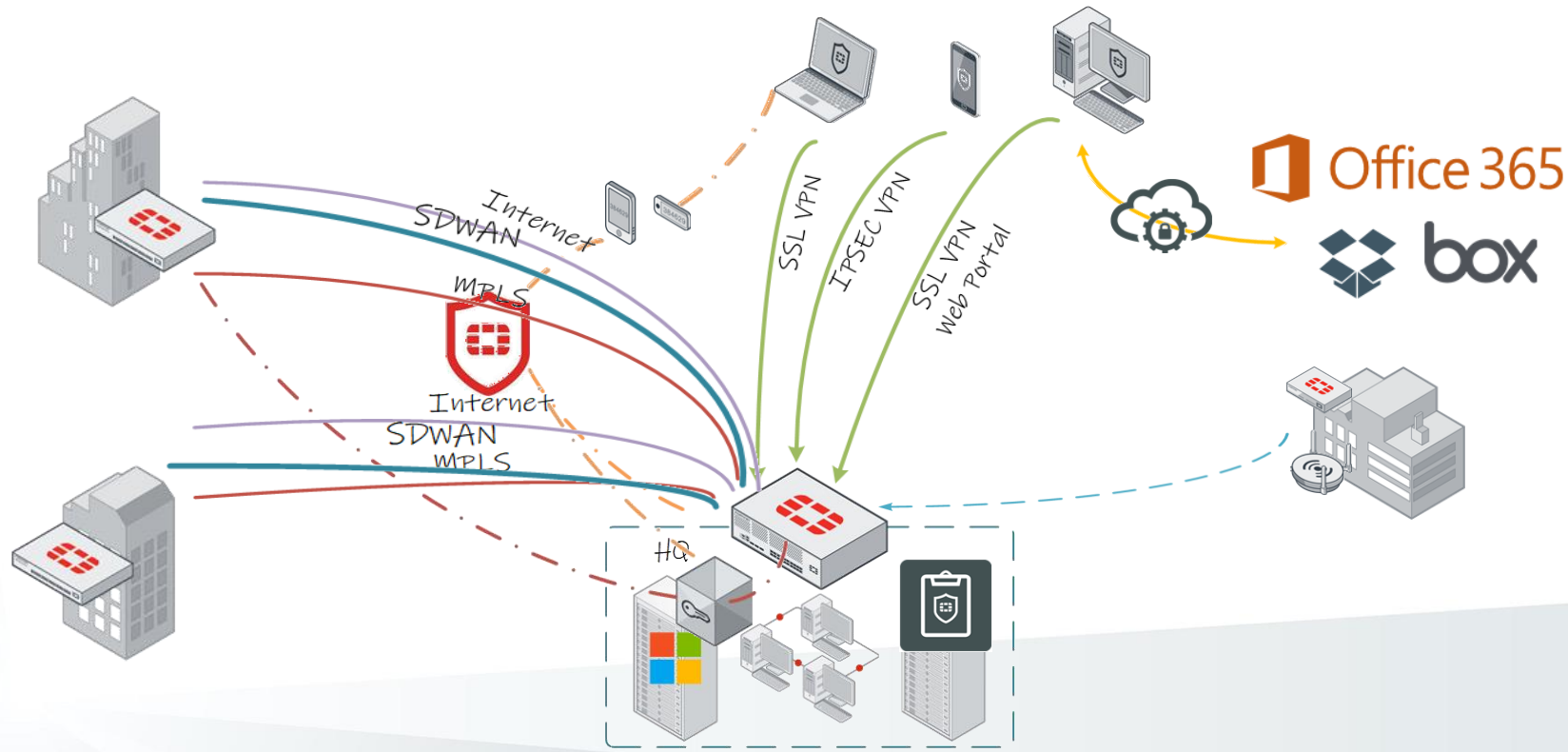


WEŹMY TO NA POWAŻNIE

CHCĘ ZBUDOWAĆ ROZWIĄZANIE BEZPIECZNEGO ZDALNEGO DOSTĘPU, ALE MUSI ONO ZAPEWNIĆ...

- WERYFIKACJĘ TOŻSAMOŚCI UŻYTKOWNIKA
- WERYFIKACJĘ URZĄDZENIA DOSTĘPOWEGO
- URUCHOMIENIE ZDALNEGO BIURA DLA ZESPOŁU UŻYTKOWNIKÓW
- PRZESYŁANIE I ANALIZĘ CAŁEGO RUCHU UŻYTKOWNIKA
- ANALIZĘ RUCHU DO USŁUG SAAS
- BEZPIECZNĄ KOMUNIKACJĘ DO WSZYSTKICH MOICH ODDZIAŁÓW
- MOŻLIWOŚĆ PRZENIESIENIA DO CHMURY

WEŹMY TO NA POWAŻNIE





Dziękujemy za uwagę

Adam Łobodziński

alobodzinski@betacom.com.pl

Wojciech Ciesielski

wciesielski@fortinet.com

