OPIS ROZWIĄZANIA

Bezpieczny dostęp zdalny dla pracowników administracji

Streszczenie

Administracje krajowe stoją w obliczu wielu różnych potencjalnych sytuacji kryzysowych, takich jak choroby, powodzie, huragany i przerwy w dostawie prądu. W takich przypadkach muszą zatem działać jako centrum koordynacji i zarządzania oraz komunikować się z obywatelami w sposób otwarty i transparentny. Wdrożenie planu ciągłości biznesowej jest niezbędne do tego, aby administracja była zdolna do działania w przypadku niesprzyjających okoliczności oraz przygotowana na potencjalne katastrofy. Nastały bowiem nowe czasy, w których pracownicy administracji mogą musieć pracować zdalnie.

Instytucje przygotowujące plan ciągłości biznesowej muszą zakładać, że nie będą mogły wykonywać zwykłej działalności w dotychczasowych obiektach. Zdolność do umożliwienia pracownikom pracy zdalnej jest niezbędna w celu zagwarantowania zarówno ciągłości działania, jak i bezpieczeństwa. Firma Fortinet oferuje w tym kontekście zintegrowane rozwiązanie do skalowalnej obsługi pracy zdalnej. Zapory sieciowe następnej generacji (NGFW) FortiGate mają wbudowane funkcje obsługi wirtualnych sieci prywatnych (VPN) opartych na protokołach SSL i IPsec, aby umożliwić pracownikom zdalnym bezpieczne połączenie z siecią danej instytucji bez konieczności wykupienia dodatkowych licencji. Dzięki ochronie urządzeń końcowych realizowanej przez rozwiązanie FortiClient oraz uwierzytelnianiu wieloskładnikowemu (MFA) realizowanemu przez rozwiązanie FortiAuthenticator, instytucja może bezpiecznie obsługiwać pracowników zdalnych i utrzymywać ciągłość biznesową.

Zdolność do bezpiecznej obsługi pracowników zdalnych jest ważnym elementem planu zapewnienia ciągłości biznesowej i odzyskiwania po awarii w każdej instytucji. Instytucja może być bowiem niezdolna do umożliwienia pracownikom zwykłej pracy na miejscu z powodu przerwy w dostawie prądu lub podobnego zdarzenia, a także wskutek epidemii lub powodzi, które mogą sprawić, że przyjeżdżanie pracowników do pracy może okazać się dla nich niebezpieczne.

W takich sytuacjach instytucja musi być zdolna do zagwarantowania bezpiecznego zdalnego dostępu do swojej sieci. 400 tys. klientów Fortinet może już korzystać z takich funkcji, zapory następnej generacji (NGFW) FortiGate obsługują bowiem wirtualne sieci prywatne oparte na protokołach SSL i IPsec, dając pracownikom zdalnym bezpieczny dostęp do sieci korporacyjnej.

Ochrona zdalnego dostępu pracowników administracji za pomocą zapór następnej generacji (NGFW) FortiGate

Rozwiązania Fortinet zostały zaprojektowane tak, aby były łatwe w użyciu i aktualizacji. Zapory następnej generacji (NGFW) FortiGate oferują funkcję bezobsługowego wdrożenia, aby zapewnić ciągłość działalności i obsługę telepracy. Pozwala to na szybkie wdrażanie urządzeń w oddziałach z minimalną konfiguracją wstępną, automatyczne pobieranie stosownych ustawień konfiguracyjnych za pośrednictwem bezpiecznych łączy oraz dokończenie konfiguracji po podłączeniu urządzeń do sieci w oddziale.

Zintegrowana z każdą zaporą następnej generacji (NGFW) FortiGate wirtualna sieć prywatna (VPN) oferuje niezwykle elastyczny model wdrożenia. Pracownicy zdalni mogą korzystać z rozwiązań niewymagających instalacji klienta albo uzyskiwać dostęp do dodatkowych funkcji za pomocą klienta VPN wbudowanego w rozwiązanie zabezpieczające urządzenia końcowe FortiClient. Użytkownicy zaawansowani i użytkownicy wykonawczy z administracji skorzystaliby na wdrożeniu punktu dostępowego FortiAP lub zapory następnej generacji FortiGate, ponieważ uzyskaliby dodatkowe funkcje.

Architektura Fortinet Security Fabric korzysta ze wspólnego systemu operacyjnego Fortinet oraz otwartego środowiska API, aby utworzyć szeroką, zintegrowaną i zautomatyzowaną architekturę zabezpieczeń. Dzięki architekturze Fortinet Security Fabric można monitorować wszystkie urządzenia instytucji (w tym urządzenia wdrożone w poszczególnych oddziałach) oraz zarządzać nimi z poziomu jednej konsoli. Za pośrednictwem wspomnianej zapory następnej generacji (NGFW) FortiGate lub scentralizowanej platformy zarządzania FortiManager wdrożonej w siedzibie instytucji zespół ds. bezpieczeństwa może uzyskać pełną widoczność wszystkich korzystających z sieci urządzeń i użytkowników, bez względu na stan wdrożenia.

W przypadku klęski żywiołowej lub innego zdarzenia zakłócającego zwykłą działalność biznesową instytucja musi być zdolna do szybkiego wdrożenia modelu pełnej pracy zdalnej. W tabeli 1 przedstawiono liczbę jednoczesnych użytkowników wirtualnej sieci prywatnej, którą mogą obsługiwać poszczególne modele zapory następnej generacji (NGFW) FortiGate.

Rozwiązania Fortinet oferują nie tylko szyfrowanie danych przesyłanych za pośrednictwem połączeń VPN, ale również szereg innych funkcji pomagających instytucjom w zabezpieczeniu pracy zdalnej. Można wśród nich wymienić:

- **Uwierzytelnianie wieloskładnikowe (MFA)**.Rozwiązania FortiToken i FortiAuthenticator oferują uwierzytelnianie dwuskładnikowe pracowników zdalnych.
- **Ochrona przed utratą danych (DLP)**. Rozwiązania FortiGate i FortiWiFi chronią przed utratą danych pracowników zdalnych, co jest niezbędne zwłaszcza w przypadku pracujących zdalnie członków ścisłego kierownictwa, którzy często mają do czynienia z wrażliwymi danymi instytucji.
- **Zabezpieczenia punktów końcowych.** Rozwiązanie FortiEDR zapewnia ochronę przed zaawansowanymi zagrożeniami komputerów pracowników zdalnych, w tym zautomatyzowane funkcje eliminowania skutków zagrożeń.
- **Ochrona przed zaawansowanymi zagrożeniami**. Rozwiązanie FortiSandbox umożliwia analizę złośliwego oprogramowania i innych podejrzanych treści w bezpiecznym środowisku testowym, zanim takie treści dotrą do miejsca przeznaczenia.
- **Łączność bezprzewodowa**. Punkty dostępowe FortiAP oferują bezpieczny dostęp bezprzewodowy w oddziałach z pełną integracją i zarządzaniem konfiguracją z poziomu jednej konsoli.
- **Zarządzanie dostępem urządzeń.** Rozwiązanie FortiNAC może egzekwować zasady związane z korzystaniem do celów służbowych z urządzeń prywatnych (BYOD) nawet za pośrednictwem zdalnych łączy VPN, co pozwala instytucji na kontrolę typów urządzeń podłączanych do sieci i przyznawanych im uprawnień dostępu.

- **Telefonia**. FortiFone to bezpieczne rozwiązanie VoIP (Voice over IP), po wdrożeniu którego ruch jest zabezpieczony, zarządzany i monitorowany przez zaporę następnej generacji (NGFW) FortiGate. Rozwiązanie to jest dostępne w postaci telefonu programowego i kilku modeli sprzętowych.

Przypadki zastosowania produktów Fortinet obsługujących pracę zdalną administracji

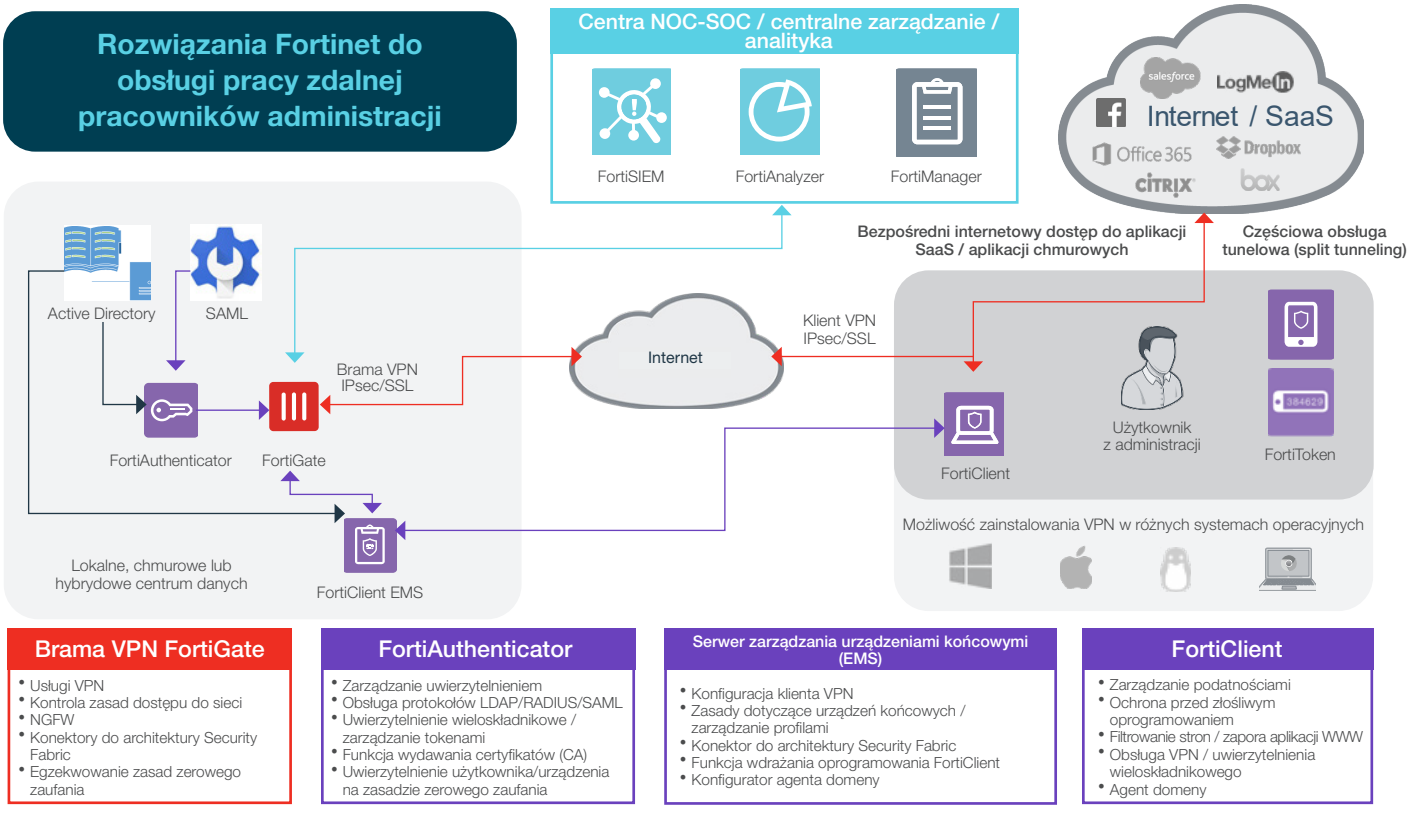
Nie każdy pracownik administracji potrzebuje tego samego poziomu dostępu do zasobów podczas pracy zdalnej, firma Fortinet oferuje zatem rozwiązania dostosowane do potrzeb każdego takiego pracownika.

Model	Jednocześni użytkownicy sieci VPN opartej na SSL	Jednocześni użytkownicy sieci VPN opartej na IPsec	Zarządzane punkty dostępowe FortiAP (tryb tunelowy)
100E	500	10 000	32
100F	500	16 000	64
600E	10 000	50 000	512
1100E	10 000	100 000	2 048
2000E	30 000	100 000	2 048
Wszystkie wyższe modele*	30 000	100 000	2 048
* Model 3300E obsługuje 1024 punkty dostępowe obsługujące tryb tunelowy			

Tabela 1. Liczba jednoczesnych połączeń wirtualnej sieci prywatnej obsługiwanych przez różne modele zapór następnej generacji (NGFW) FortiGate.

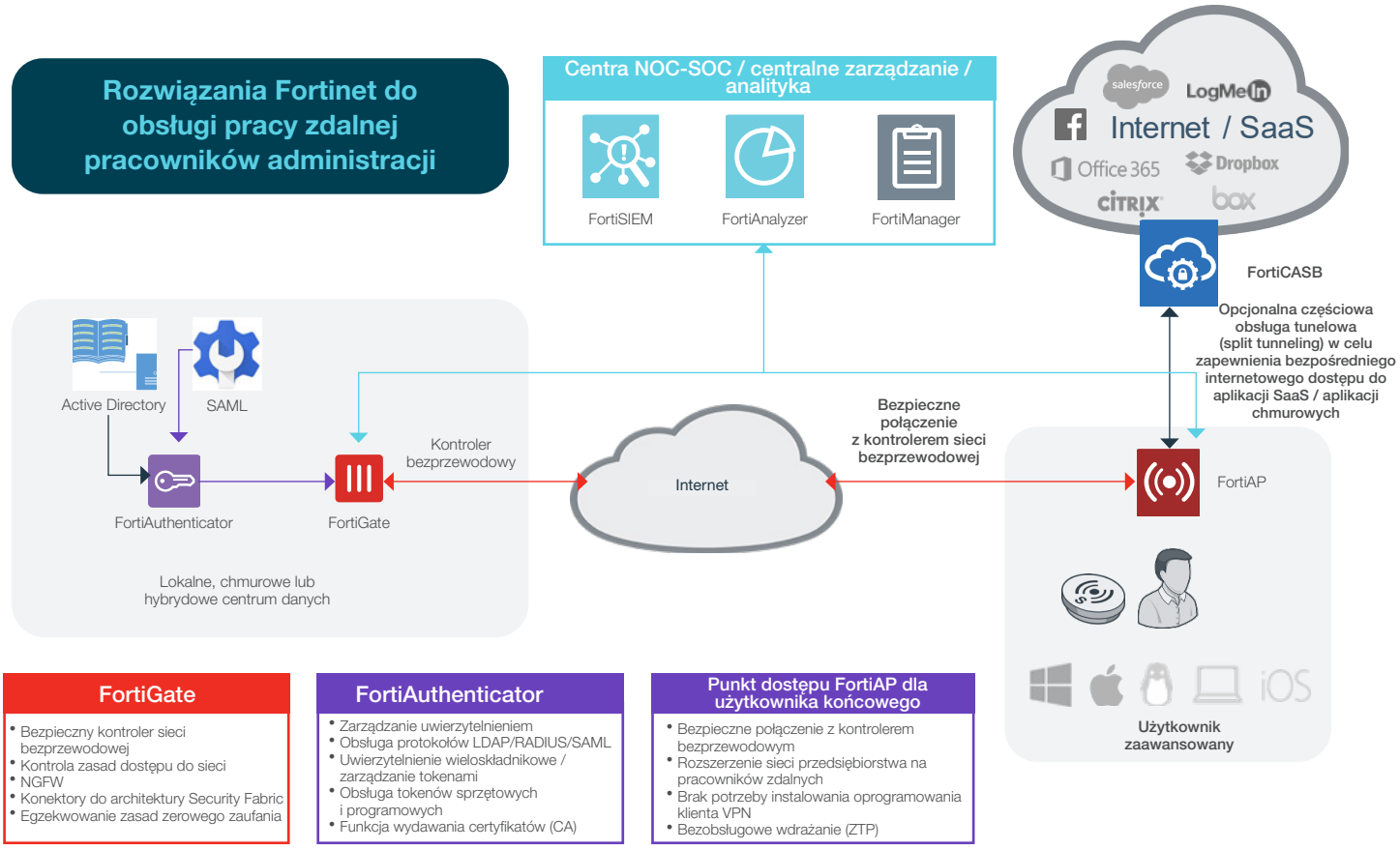
1. **Podstawowy pracownik zdalny administracji (telepracownik).** Podstawowym telepracownikom potrzebny jest podczas pracy zdalnej jedynie dostęp do poczty elektronicznej, Internetu i funkcji telekonferencyjnych, ograniczona możliwość przesyłania plików oraz dostęp do funkcji właściwych dla danego stanowiska pracy (kadry itp.), w tym dostęp do aplikacji SaaS (oprogramowanie jako usługa) w chmurze, na przykład aplikacji Microsoft Office 365, oraz bezpieczne połączenie z siecią administracji.

   Podstawowi telepracownicy mogą łączyć się z siecią instytucji za pomocą zintegrowanego oprogramowania klienckiego VPN FortiClient i weryfikować swoją tożsamość w ramach oferowanych przez rozwiązanie FortiToken funkcji uwierzytelniania wieloskładnikowego.



Rysunek 1. Wdrożenie rozwiązania Fortinet dla podstawowego pracownika zdalnego administracji.

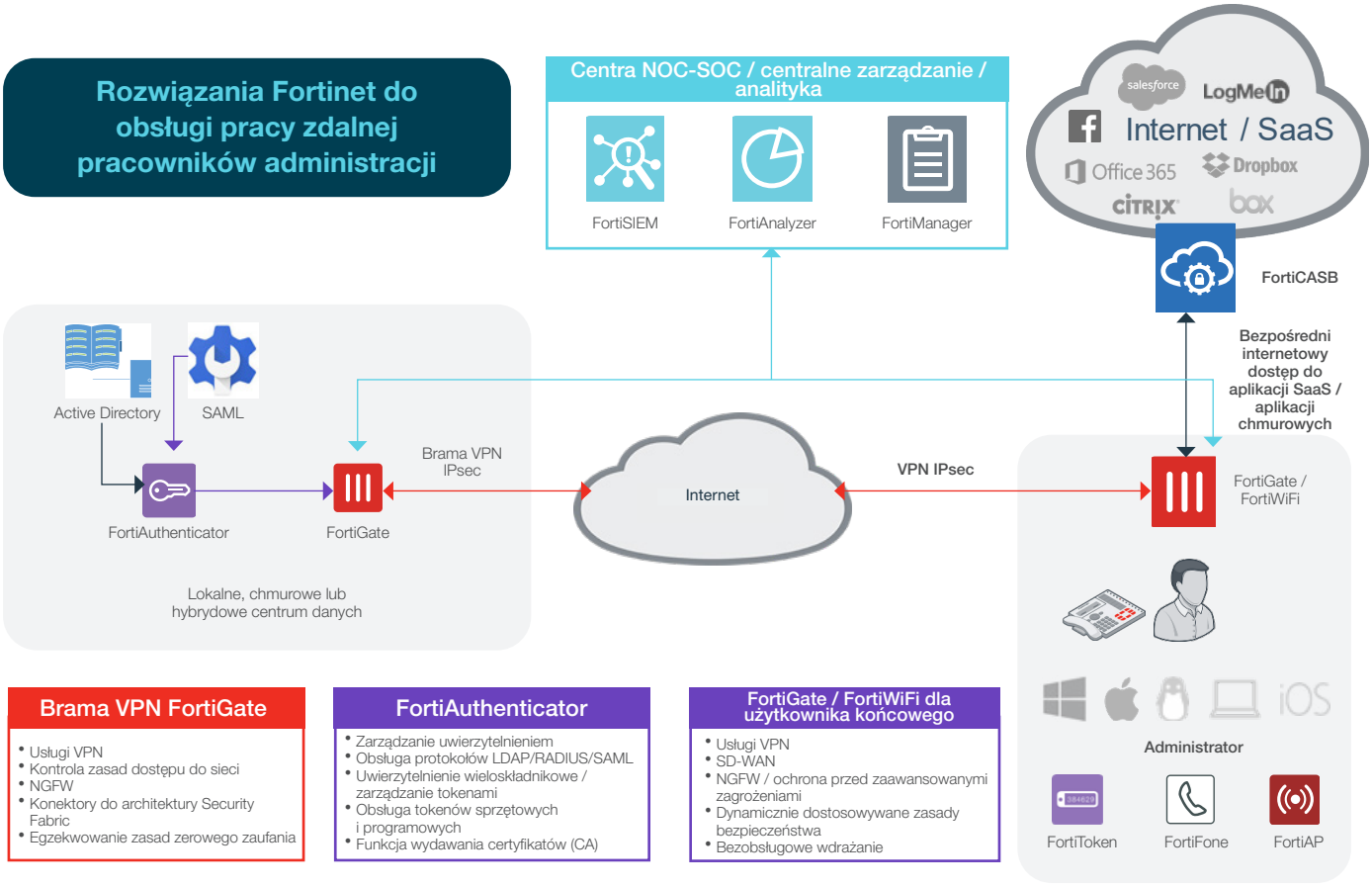
2. **Użytkownik zaawansowany (ang. power user) z administracji.** Użytkownicy zaawansowani to pracownicy administracji, którym podczas pracy zdalnej potrzebny jest wyższy poziom dostępu do zasobów danej instytucji, na przykład w celu korzystania z wielu równoległych środowisk IT. Użytkownikami zaawansowanymi mogą być administratorzy systemów, inżynierowie IT oraz personel awaryjny. W przypadku użytkowników zaawansowanych wdrożenie punktu dostępowego FortiAP w miejscu ich pracy zdalnej da im odpowiedni poziom dostępu i bezpieczeństwa. Punkt taki zagwarantuje bezpieczną łączność bezprzewodową za pośrednictwem trwałego, bezpiecznego tunelu prowadzącego do sieci danej instytucji. Punkty dostępowe FortiAP mogą być wdrażane w ramach bezobsługowej instalacji i zarządzane z biura za pomocą zapory następnej generacji (NGFW) FortiGate. W przypadku konieczności zainstalowania telefonu po prostu podłącza się go do punktu dostępowego FortiAP, aby działał tak, jakby było się w biurze.



Rysunek 2. Hipotetyczne wdrożenie rozwiązania Fortinet dla użytkownika zaawansowanego z administracji.

3. **Administrator z administracji.** Administrator to pracownik, który nawet podczas pracy zdalnej potrzebuje zaawansowanego dostępu do poufnych zasobów instytucji oraz często przetwarza wrażliwe i tajne informacje. Ten profil pracownika obejmuje administratorów z uprzywilejowanym dostępem do systemu, inżynierów pomocy technicznej, kluczowych partnerów administracji i kluczowe instytucje w kontekście planu ciągłości działania, personel awaryjny oraz urzędników takich jak dyrektorów agencji rządowych, gubernatorów, burmistrzów oraz podległy im personel.

   Miejsce pracy zdalnej takiego administratora powinno mieć charakter lokalizacji zapasowej dla biura. Administratorom potrzebne będą również wszystkie funkcje dostępne podstawowym pracownikom zdalnym administracji i użytkownikom zaawansowanym oraz określone funkcje dodatkowe. W tym celu punkt dostępowy FortiAP można zintegrować z zaporą następnej generacji (NGFW) FortiGate lub rozwiązaniem FortiWiFi, aby zagwarantować administratorom bezpieczną łączność bezprzewodową z wbudowanymi funkcjami ochrony przed utratą danych (DLP). Rozwiązanie FortiFone oferuje natomiast telefon programowy lub sprzętowe wersje telefonii VoIP zarządzane i zabezpieczone za pośrednictwem zapory następnej generacji (NGFW) FortiGate wdrożonej lokalnie lub platformy scentralizowanego zarządzania FortiManager wdrożonej w biurze.



Rysunek 3. Hipotetyczne wdrożenie rozwiązania Fortinet dla administratora z administracji.

Pełna integracja zabezpieczeń dzięki rozwiązaniom Fortinet

Architektura Fortinet Security Fabric umożliwia niezawodną integrację pracowników zdalnych z administracji. Wszystkie rozwiązania Fortinet są ze sobą połączone za pośrednictwem architektury Fortinet Security Fabric, co oferuje widoczność oraz możliwości konfiguracji i monitorowania z poziomu jednej konsoli. Ponadto szereg konektorów do architektury Fabric, otwarte środowisko API, wsparcie społeczności DevOps i rozbudowany ekosystem architektury Security Fabric umożliwiają integrację z ponad 250 rozwiązaniami innych producentów.

Jest to niezbędne wówczas, gdy administracja przygotowuje plan ciągłości biznesowej, ponieważ może być zmuszona do całkowitego przejścia na pracę zdalną z niewielkim lub żadnym wyprzedzeniem. Ponadto funkcje zapewnienia widoczności i zarządzania architekturą zabezpieczeń gwarantują, że obsługa telepracy nie naraża na szwank cyberbezpieczeństwa danej instytucji.

Poniższe rozwiązania wchodzą w skład architektury Fortinet Security Fabric i obsługują bezpieczną pracę zdalną:

- **FortiClient**. FortiClient wzmacnia bezpieczeństwo urządzeń końcowych dzięki zapewnieniu zintegrowanej widoczności, kontroli i proaktywnej ochrony oraz umożliwia instytucji wykrywanie, monitorowanie i ocenę ryzyka dla urządzeń końcowych w czasie rzeczywistym.
- **FortiGate (BYOL, PAYG)**. Zapora następnej generacji (NGFW) FortiGate korzysta ze specjalnych procesorów obsługujących funkcje zabezpieczeń, aby zagwarantować najwyższej klasy ochronę, kompleksową widoczność i scentralizowaną kontrolę oraz wydajną weryfikację ruchu szyfrowanego i nieszyfrowanego.
- **FortiWiFi**. Bramy do sieci bezprzewodowej FortiWiFi łączą w sobie zalety zabezpieczeń zapory następnej generacji (NGFW) FortiGate z punktem dostępu do sieci bezprzewodowej, oferując zintegrowane rozwiązanie sieciowe i zabezpieczające dla telepracowników.
- **FortiFone**. FortiFone oferuje jednolitą komunikację głosową za pośrednictwem protokołu VoIP, która jest zabezpieczona i zarządzana przez zapory następnej generacji (NGFW) FortiGate. Interfejs telefonu programowego FortiFone umożliwia wykonywanie i odbieranie połączeń, dostęp do poczty głosowej, sprawdzanie historii połączeń i przeszukiwanie katalogu przedsiębiorstwa bezpośrednio z urządzenia przenośnego. Dostępnych jest też wiele modeli sprzętowych.
- **FortiToken**. FortiToken potwierdza tożsamość użytkowników przez dodanie drugiego składnika procesu uwierzytelniania w ramach fizycznych lub mobilnych tokenów opartych o aplikacje.

- **FortiAuthenticator**. FortiAuthenticator oferuje scentralizowane usługi uwierzytelniania, w tym usługi jednokrotnego logowania, zarządzania certyfikatami i zarządzania gośćmi.
- **FortiAP**. Punkt dostępowy FortiAP oferuje bezpieczny dostęp bezprzewodowy do rozproszonych instytucji i pracowników zdalnych oraz może być łatwo zarządzany za pośrednictwem zapory następnej generacji (NGFW) FortiGate lub chmury.
- **FortiWeb Cloud (BYOL, PAYG).** Oferowana przez Fortinet zapora aplikacji WWW (WAF) chroni hostowane aplikacje WWW przed zarówno znanymi, jak i nieznanymi zagrożeniami za pomocą wielowarstwowych i skorelowanych metod wykrywania ataków.
- **FortiManager (BYOL)**. FortiManager umożliwia zarządzanie i kontrolę zasad w całym rozszerzonej instytucji z poziomu jednej konsoli w celu uzyskania informacji na temat dotyczących całej sieci zagrożeń opartych na ruchu. Obejmuje to funkcje zapobiegające zaawansowanym atakom oraz funkcje skalowania umożliwiające zarządzanie nawet 10 tys. urządzeń Fortinet.
- **FortiAnalyzer (BYOL)**. FortiAnalyzer oferuje oparte na wynikach analizy danych cyberzabezpieczenia oraz funkcje zarządzania dziennikami umożliwiające lepsze wykrywanie zagrożeń i zapobieganie naruszeniom.
- **FortiSandbox (BYOL, PAYG)**. Bezpieczne środowisko testowe Fortinet oferuje wydajną kombinację funkcji elastycznego wdrażania, zbierania informacji oraz zaawansowanego wykrywania i łagodzenia skutków zagrożeń w celu zapobiegania ukierunkowanym atakom i utracie danych oraz neutralizowania skutków tych zdarzeń.

Bezpieczna infrastruktura zapewnia ciągłość biznesową.

Zagwarantowanie ciągłości biznesowej i możliwości odzyskiwania danych po awarii jest niezbędne w każdej instytucji. Ważnym składnikiem tego procesu jest zdolność do natychmiastowej obsługi większości lub wszystkich pracowników zdalnych.

Przygotowując plany ciągłości biznesowej, należy zatem upewnić się, że instytucja dysponuje odpowiednimi zasobami pozwalającymi na ochronę pracowników zdalnych. Rozwiązania Fortinet są łatwe we wdrożeniu i konfigurowaniu oraz umożliwiają instytucjom zagwarantowanie pełnego bezpieczeństwa, widoczności i kontroli niezależnie od środowiska wdrożenia.

listopada10,20214:24PM

635636-0-0-PL

sb-FA-secure-remote-access-for-your-government-workforce-482020-a4_PL