OPIS ROZWIĄZANIA

Bezpieczny dostęp zdalny dla wszystkich pracowników

Streszczenie

Przedsiębiorstwa stoją w obliczu wielu różnych potencjalnych sytuacji kryzysowych, takich jak choroby, powodzie, huragany i przerwy w dostawie prądu. Wdrożenie planu ciągłości biznesowej jest niezbędne do tego, aby przedsiębiorstwo było zdolne do utrzymania ruchu w przypadku niesprzyjających okoliczności oraz przygotowane na potencjalne katastrofy.

Przedsiębiorstwa 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 obsługi pracy zdalnej. Zapory sieciowe następnej generacji (NGFW) FortiGate mają wbudowane funkcje obsługi wirtualnych sieci prywatnych (VPN) opartych na protokole IPsec, aby umożliwić pracownikom zdalnym bezpieczne połączenie z siecią przedsiębiorstwa. Dzięki ochronie urządzeń końcowych realizowanej przez rozwiązanie FortiClient oraz uwierzytelnianiu wieloskładnikowemu (MFA) realizowanemu przez rozwiązanie FortiAuthenticator, przedsiębiorstwo może bezpiecznie obsługiwać pracowników zdalnych i utrzymywać ciągłość biznesową.

Zdolność do bezpiecznej obsługi pracowników zdalnych jest ważnym elementem planuciągłościbiznesowej i odzyskiwania po awarii w każdym przedsiębiorstwie. Przedsiębiorstwo może być bowiem niezdolne 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 przedsiębiorstwo musi być zdolne do zagwarantowania bezpiecznego zdalnego dostępu do swojej sieci. 400 tys. klientów Fortinet może już korzystać z takich funkcji, zapory następnej generacji FortiGate obsługują bowiem wirtualne sieci prywatne oparte na protokole IPsec, dając pracownikom zdalnym bezpieczny dostęp do sieci korporacyjnej.

Praca zdalna skraca czas bezproduktywności pracownika średnio o 27%[1].

Pracownicy zdalni pracują rocznie średnio o 16,8 dnia więcej niż pracownicy zatrudnieni na miejscu[2].

85% pracowników twierdzi, że maksymalną produktywność osiąga podczas pracy zdalnej[3].

Umożliwienie pracy zdalnej zwiększyło zdolność do zatrzymania pracowników w 95% przedsiębiorstw[4].

Zabezpieczenie zdalnego dostępu do sieci za pomocą zapór następnej generacji FortiGate

Zintegrowane z każdą zaporą następnej generacji FortiGate wirtualne sieci prywatne oparte na protokole IPsec lub SSL oferują 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 administratorzy skorzystaliby na wdrożeniu punktu dostępowego FortiAP lub zapory następnej generacji FortiGate, ponieważ uzyskaliby dodatkowe funkcje.

Rozwiązania Fortinet zostały zaprojektowane tak, aby były łatwe w użyciu od momentu ich pierwszego zakupu do końca cyklu ich eksploatacji. Zapory następnej generacji FortiGate i punkty dostępu bezprzewodowego FortiAP oferują funkcję bezobsługowego wdrożenia. Urządzenia wdrażane w odległych lokalizacjach mogą być przed wysyłką wstępnie skonfigurowane, aby ułatwić automatyczną konfigurację na miejscu i zapewnić ciągłość działalności i obsługę telepracy.

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 przedsiębiorstwa (w tym urządzenia wdrożone w poszczególnych oddziałach) oraz zarządzać nimi z poziomu jednej konsoli. Za pośrednictwem wspomnianej zapory następnej generacji FortiGate lub scentralizowanej platformy zarządzania FortiManager wdrożonej w siedzibie przedsiębiorstwa zespół ds. bezpieczeństwa może uzyskać pełną widoczność wszystkich podłączonych do sieci urządzeń, bez względu na stan ich wdrożenia.

W przypadku klęski żywiołowej lub innego zdarzenia zakłócającego zwykłą działalność biznesową przedsiębiorstwo musi być zdolne 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 FortiGate.

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

- **Uwierzytelnianie wieloskładnikowe**. 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 przedsiębiorstwa.

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

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
300E	5000	50 000	256
500E	10 000	50 000	256
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			

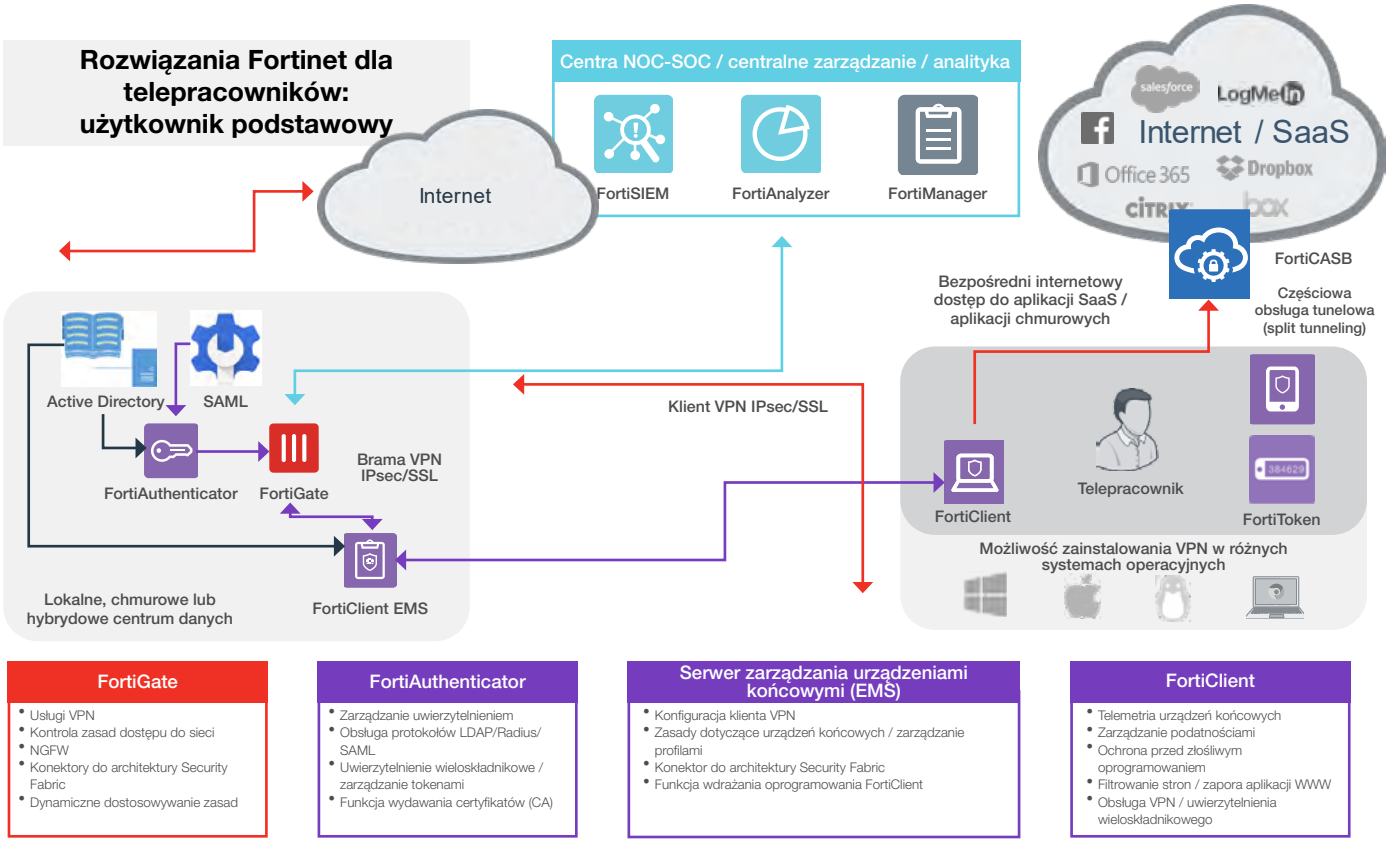
Tabela 1. Liczba jednoczesnych połączeń wirtualnej sieci prywatnej obsługiwanych przez różne modele zapór następnej generacji FortiGate.

Przypadki zastosowania produktów Fortinet obsługujących pracę zdalną

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

1. **Podstawowy pracownik zdalny (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 (finanse, kadry itp.), w tym dostęp do aplikacji SaaS (oprogramowanie jako usługa) w chmurze, na przykład aplikacji Microsoft Office 365, oraz bezpieczne połączenie z siecią przedsiębiorstwa.

   Podstawowi telepracownicy mogą łączyć się z siecią przedsiębiorstwa za pomocą zintegrowanego oprogramowania klienckiego VPN FortiClient i weryfikować swoją tożsamość w ramach oferowanych przez rozwiązanie FortiToken funkcji uwierzytelniania wieloskładnikowego. Warto pamiętać, że gdy użytkownicy zaawansowani i administratorzy opuszczą swoje miejsce pracy zdalnej, ich profile zmienią się w profil podstawowego telepracownika.



FortiGate
- Usługi VPN
- Kontrola zasad dostępu do sieci
- NGFW
- Konektory do architektury Security Fabric
- Dynamiczne dostosowywanie zasad

FortiAuthenticator
- Zarządzanie uwierzytelnieniem
- Obsługa protokołów LDAP/Radius/SAML
- Uwierzytelnienie wieloskładnikowe / zarządzanie tokenami
- Funkcja wydawania certyfikatów (CA)

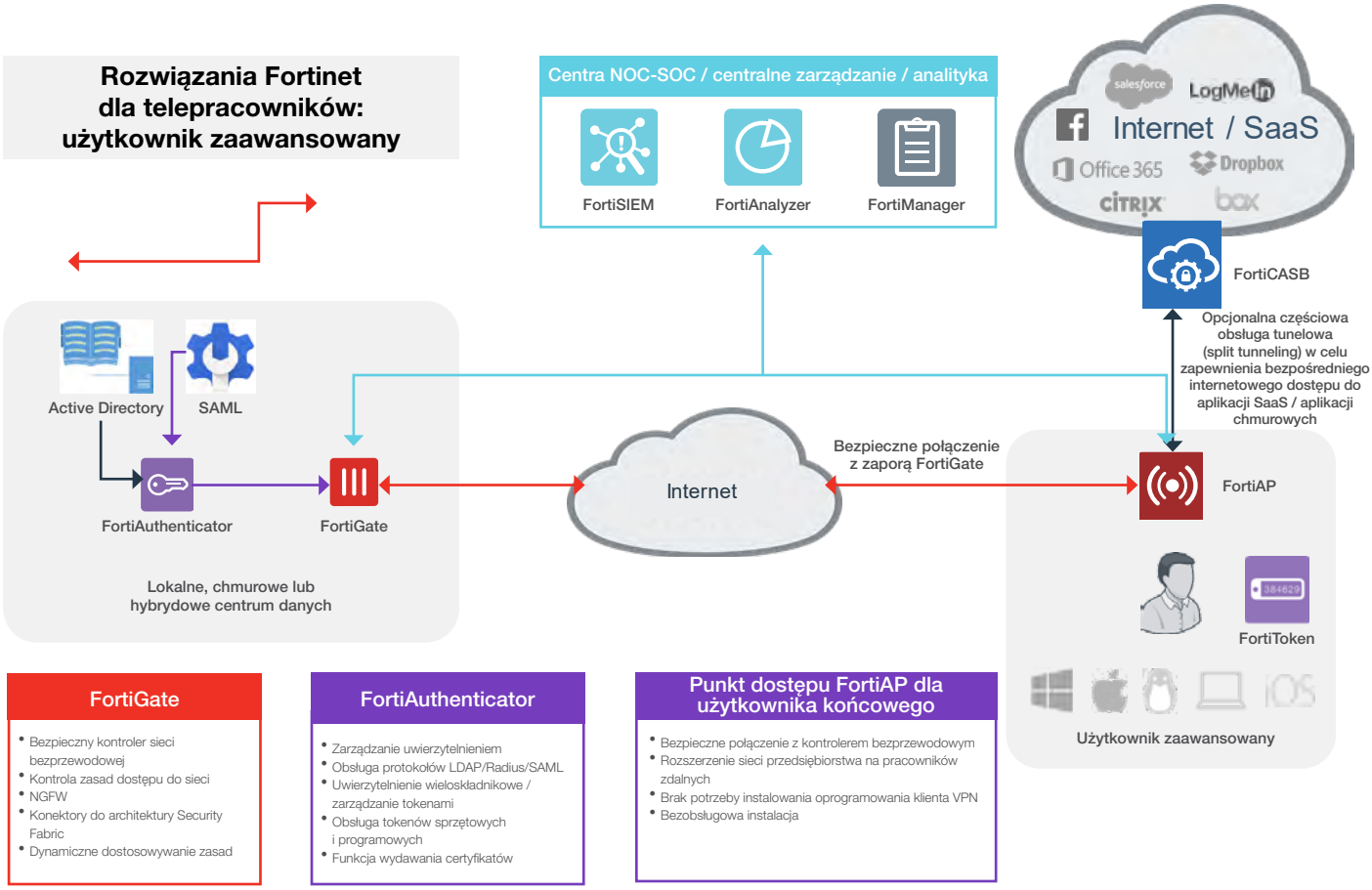
Serwer zarządzania urządzeniami końcowymi (EMS)
- Konfiguracja klienta VPN
- Zasady dotyczące urządzeń końcowych / zarządzanie profilami
- Konektor do architektury Security Fabric
- Funkcja wdrażania oprogramowania FortiClient

FortiClient
- Telemetria urządzeń końcowych
- Zarządzanie podatnościami
- Ochrona przed złośliwym oprogramowaniem
- Filtrowanie stron / zapora aplikacji WWW
- Obsługa VPN / uwierzytelnienia wieloskładnikowego

Rysunek 1. Hipotetyczne wdrożenie rozwiązania Fortinet dla podstawowego telepracownika.

2. **Użytkownik zaawansowany (ang. power user)**. Użytkownicy zaawansowani to pracownicy, którym podczas pracy zdalnej potrzebny jest wyższy poziom dostępu do zasobów przedsiębiorstwa, na przykład w celu korzystania z wielu równoległych środowisk IT. Użytkownikami zaawansowanymi mogą być administratorzy systemów, inżynierowie IT oraz personel awaryjny.

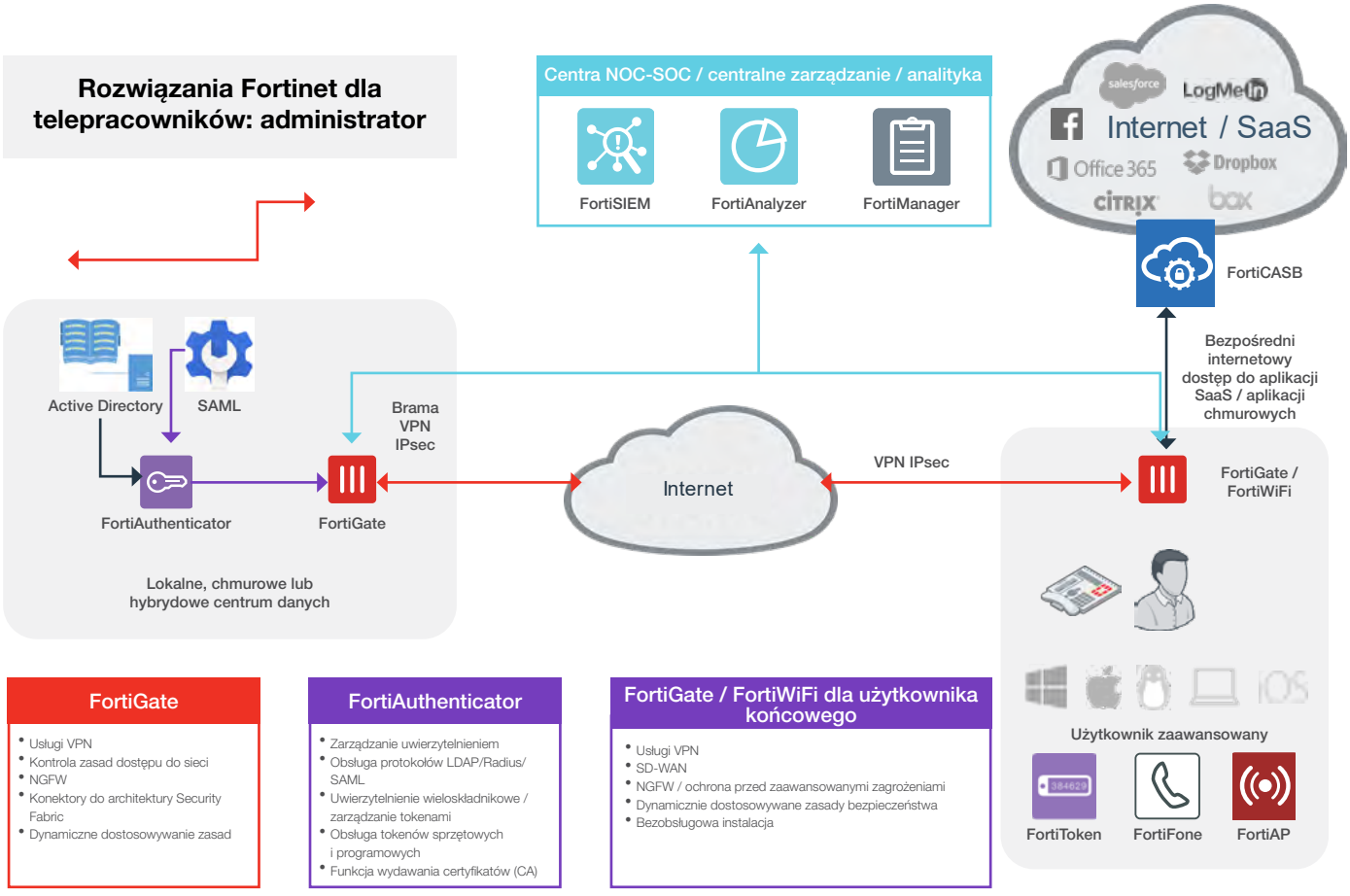
   W przypadku użytkowników zaawansowanych wdrożenie punktu dostępowego FortiAP w miejscu ich pracy zdalnej da im odpowiedni poziom dostępu i bezpieczeństwa. Punkt taki zagwarantuje bezpieczną łączność bezprzewodową za pośrednictwem bezpiecznego tunelu prowadzącego do sieci przedsiębiorstwa. Punkty dostępowe FortiAP mogą być wdrażane w ramach bezobsługowej instalacji i zarządzane z biura za pomocą zapory następnej generacji FortiGate. W przypadku konieczności zainstalowania telefonu firmowego 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.

3. **Administrator (ang. super user).** Administrator to pracownik, który nawet podczas pracy zdalnej potrzebuje zaawansowanego dostępu do poufnych zasobów przedsiębiorstwa i często przetwarza wrażliwe i tajne informacje. Ten profil pracownika obejmuje administratorów z uprzywilejowanym dostępem do systemu, inżynierów pomocy technicznej, kluczowych partnerów w kontekście planu ciągłości działania, personel awaryjny i członków ścisłego kierownictwa.

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



Rysunek 3. Hipotetyczne wdrożenie rozwiązania Fortinet dla administratora.

Obsługa pracowników zdalnych

Rozwiązania Fortinet są łatwe do wdrożenia w miejscach pracy pracowników zdalnych. Przedsiębiorstwo potrzebuje jednak również zasobów u siebie lub w chmurze, aby bezpiecznie obsługiwać telepracowników.

Wiele przedsiębiorstw dysponuje już takimi zasobami, ponieważ są one częścią istniejącej architektury zabezpieczeń. Zapora następnej generacji FortiGate jest na przykład zdolna do kontroli zaszyfrowanego i niezaszyfrowanego ruchu sieciowego w ramach całego przedsiębiorstwa przy minimalnym wpływie na wydajność sieci. Obejmuje również zintegrowaną bramę VPN, która działa jak urządzenie końcowe oferujące szyfrowane połączenia z telepracownikami.

Zapora następnej generacji FortiGate może być również zintegrowana z typową infrastrukturą IT, w tym z korporacyjnymi usługami katalogowymi, takimi jak Microsoft Active Directory (AD), oraz funkcjami uwierzytelniania dwuskładnikowego (MFA) i jednokrotnego logowania (SSO). FortiAuthenticator udostępnia jeden, scentralizowany punkt integracji dla narzędzi uwierzytelniających oraz obsługuje zarówno rozwiązania innych firm, jak i rozwiązanie FortiToken, które oferuje opcje tokenów sprzętowych, programowych, pocztowych i mobilnych.

W kontekście zarządzania pracownikami zdalnymi znajdującymi się w różnych lokalizacjach niezbędne stają się funkcje oferujące scentralizowaną widoczność zabezpieczeń i scentralizowane nimi zarządzanie. Wszystkie rozwiązania Fortinet można zintegrować za pośrednictwem architektury Fortinet Security Fabric. W rezultacie dział IT może za pomocą programu FortiManager uzyskać niezbędną widoczność i kontrolę z poziomu jednej konsoli, za pomocą programu FortiAnalyzer agregować dzienniki danych sieciowych i wykonywać analizy bezpieczeństwa oraz za pomocą programu FortiSIEM szybko wykrywać i reagować na potencjalne zagrożenia.

Pełna integracja zabezpieczeń dzięki rozwiązaniom Fortinet

Architektura Fortinet Security Fabric umożliwia niezawodną integrację pracowników zdalnych. 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 firm.

Jest to niezbędne wówczas, gdy przedsiębiorstwo przygotowuje plan ciągłościbiznesowej, ponieważ może być ono zmuszone do całkowitego przejścia na pracę zdalną z niewielkim lub żadnym wyprzedzeniem. Ponadto funkcje zapewnienia widoczności i zarządzania architekturą zabezpieczeń w przedsiębiorstwie gwarantują, że obsługa telepracy nie naraża na szwank cyberbezpieczeństwa przedsiębiorstwa.

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 przedsiębiorstwom wykrywanie, monitorowanie i ocenę ryzyka dla urządzeń końcowych w czasie rzeczywistym.
- **FortiGate**. Zapora następnej generacji 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 FortiGate z punktem dostępu do sieci bezprzewodowej, oferując zintegrowane rozwiązanie sieciowe i zabezpieczające dla telepracowników.
- **FortiFone**. FortiFone zapewnia jednolitą komunikację głosową za pośrednictwem protokołu VoIP, która jest zabezpieczona i zarządzana przez zapory następnej generacji FortiGate. Interfejs telefonu internetowego 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 opcji 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 zapewnia bezpieczny dostęp bezprzewodowy do rozproszonych przedsiębiorstw i pracowników zdalnych i może być łatwo zarządzany za pośrednictwem zapory następnej generacji FortiGate lub chmury.
- **FortiManager**. FortiManager umożliwia zarządzanie i kontrolę zasad w całym rozszerzonym przedsiębiorstwie 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**. FortiAnalyzer oferuje oparte na wynikach analizy danych cyberzabezpieczenia oraz funkcje zarządzania dziennikami umożliwiające lepsze wykrywanie zagrożeń i zapobieganie naruszeniom.
- **FortiSandbox**. 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. Środowisko to jest oferowane jako usługa chmurowa, która jest zawarta w większości subskrypcji FortiGuard.

Bezpieczna infrastruktura zapewnia ciągłość biznesową.

Zagwarantowanie ciągłościbiznesowej i możliwości odzyskiwania danych po awarii jest niezbędne w każdym przedsiębiorstwie. Ważnym składnikiem tego procesu jest zdolność do natychmiastowej obsługi większości lub wszystkich pracowników zdalnych.

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

1 „The Benefits of Working From Home", Airtasker, 9 września 2019 r.

2 Ibid.

3 Abdullahi Muhammed, „Here's Why Remote Workers Are More Productive Than In-House Teams", Forbes, 21 maja 2019 r.

4 Ibid.

3 czerwca 2020, 04:00

618770-0-1-PL

sb-FA-secure-remote-access-for-your-workforce-at-scale-3132020_A4_PL