IBM Security Verify

Niniejszy opis dotyczy Usługi Przetwarzania w Chmurze. Odpowiednie dokumenty zamówienia zawierają ceny i dodatkowe informacje dotyczące zamówienia Klienta.

1. Usługa Przetwarzania w Chmurze

W ramach usługi IBM Cloud Identity dostępne są funkcje pojedynczego logowania i uwierzytelniania wieloskładnikowego oraz mechanizmy zarządzania cyklem życia tożsamości użytkowników wewnętrznych (pracowników) i zewnętrznych.

1.1 Produkty oferowane

Klient może dokonać wyboru spośród następujących produktów oferowanych.

1.1.1 IBM Security Verify

IBM Security Verify pomaga Klientom w zapewnieniu większej produktywności użytkowników dzięki takim funkcjom dostępnym w chmurze, jak pojedyncze logowanie, uwierzytelnianie wieloskładnikowe, zarządzanie cyklem życia, uwierzytelnianie adaptacyjne, analiza tożsamości i nadzór nad tożsamością, w ramach produktu o jednym numerze katalogowym. Ta Usługa Przetwarzania w Chmurze obsługuje również tysiące gotowych konektorów, które ułatwiają dostęp do popularnych aplikacji w chmurze, oraz gotowe szablony pomagające w integrowaniu własnych aplikacji przedsiębiorstwa.

- Pojedyncze logowanie

  Ta Usługa Przetwarzania w Chmurze udostępnia funkcje pojedynczego logowania i OpenID Connect (OIDC), uwierzytelnianie jako usługę do obsługi autoryzacji za pomocą funkcji API w chmurze, starter aplikacji, raporty administracyjne i analityczny panel kontrolny. Usługa łączy użytkowników i aplikacje z wykorzystaniem uwierzytelniania opartego na nowoczesnych standardach oraz protokołów stowarzyszania. Uwzględnia setki konektorów do powszechnie używanych aplikacji. Ta Usługa Przetwarzania w Chmurze jest ściśle zintegrowana z zainstalowanym lokalnie oprogramowaniem IBM Security Verify Access i oprogramowaniem IBM Security Verify Application Gateway, które jest do niej dołączone jako oprogramowanie pomocnicze. W ten sposób powstało rozwiązanie, które umożliwia pionom przedsiębiorstw Klientów zarządzanie dostępem do aplikacji zarówno zainstalowanych lokalnie, jak i działających w chmurze.

- Uwierzytelnianie wieloskładnikowe

  W ramach tej Usługi Przetwarzania w Chmurze dostępne są funkcje uwierzytelniania wieloskładnikowego w aplikacjach chronionych przez usługę Cloud Identity Connect oraz za pośrednictwem bezpośredniego wywołania funkcji API. Obsługiwane są również inne punkty kontroli dostępu, m.in. klienty RADIUS, serwery PAM z systemem Unix/Linux i serwery Windows, w celu weryfikacji tożsamości podczas uzyskiwania dostępu do usług cyfrowych. Obejmuje to takie mechanizmy jak hasła jednorazowe przesyłane pocztą elektroniczną i w wiadomości SMS oraz hasła o ograniczonym czasie ważności (znaczniki programowe), a także uwierzytelnianie biometryczne oparte na technologii push obsługiwane przez rozwiązanie IBM Verify. Ta Usługa Przetwarzania w Chmurze jest zintegrowana z zainstalowanym lokalnie oprogramowaniem IBM Security Verify Access. W ten sposób powstało rozwiązanie, które umożliwia pionom przedsiębiorstw Klientów zarządzanie dostępem do aplikacji zarówno zainstalowanych lokalnie, jak i działających w chmurze.

- Dostęp adaptacyjny

  Ta Usługa Przetwarzania w Chmurze, dzięki wykorzystaniu funkcji analizy zagrożeń oraz sztucznej inteligencji, ułatwia przedsiębiorstwom odróżnianie zwykłych użytkowników od użytkowników o złych zamiarach podczas uzyskiwania przez nich dostępu do aplikacji chronionej przez tę usługę. Na podstawie informacji dotyczących użytkowników oraz ich urządzeń i wzorców zachowań usługa ta umożliwia ustalenie w czasie rzeczywistym, jakie działania należy podjąć w celu zmniejszenia ryzyka: zezwolić na dostęp, domagać się uwierzytelnienia czy zablokować dostęp. W usłudze tej wykorzystywanych jest kilkaset punktów danych oraz informacje kontekstowe gromadzone z urządzenia użytkownika końcowego w celu oznaczenia urządzenia za pomocą odcisku palca i obliczenia całościowego poziomu ryzyka dla danej sesji. Reguły oceny oparte na ryzyku,

zdefiniowane w strategii dostępu, umożliwiają określenie działań systemu na podstawie poziomu ryzyka sesji oraz dodatkowych parametrów. Usługa ta jest ściśle powiązana z raportami administratora usługi Security Verify, edytorem reguł strategii dostępu oraz usługą uwierzytelniania wieloskładnikowego.

- Zarządzanie cyklem życia i nadzór

  Ta Usługa Przetwarzania w Chmurze jest ściśle zintegrowana z zainstalowanym lokalnie oprogramowaniem IBM Security Identity Governance and Intelligence (IGI) i IBM Security Identity Manager (ISIM) dołączonym do niej jako oprogramowanie pomocnicze. W ten sposób powstało rozwiązanie, które umożliwia pionom przedsiębiorstw Klientów nadzór nad tożsamością w odniesieniu do aplikacji zarówno zainstalowanych lokalnie, jak i działających w chmurze. Ta Usługa Przetwarzania w Chmurze udostępnia organizacjom zaawansowane możliwości zarządzania cyklem życia tożsamości użytkowników w środowisku chmury, takie jak synchronizacja kont, przepływ pracy dotyczący żądań dostępu do aplikacji, certyfikacja dostępu oraz udostępnianie usług w aplikacjach chmurowych i lokalnych. Klient może również dodać rozwiązanie IBM Security Verify Account Synchronization jako usługę dodatkową.

- Analiza

  Ta Usługa Przetwarzania w Chmurze wzbogaca istniejące rozwiązania IBM, takie jak IBM Security Identity Governance and Intelligence (IGI) i IBM Security Identity Manager (ISIM), co pozwala określić kompleksowy profil ryzyka dla zarządzanych użytkowników. Usługa udostępnia lokalny, wielofunkcyjny mechanizm analityczny, który przetwarza dane dotyczące działań i uprawnień pochodzące z różnych źródeł. Zapewnia to pełny obraz czynników ryzyka związanych z dostępem i daje możliwość podjęcia działań na podstawie uzyskanych informacji.

1.1.2 IBM Cloud Identity Connect

Ta Usługa Przetwarzania w Chmurze udostępnia funkcje pojedynczego logowania i OpenID Connect (OIDC), uwierzytelnianie jako usługę do obsługi autoryzacji za pomocą funkcji API w chmurze, starter aplikacji, raporty administracyjne i analityczny panel kontrolny. Usługa łączy użytkowników i aplikacje z wykorzystaniem uwierzytelniania opartego na nowoczesnych standardach oraz protokołów stowarzyszania. Uwzględnia setki konektorów do powszechnie używanych aplikacji. Ta Usługa Przetwarzania w Chmurze jest ściśle zintegrowana z zainstalowanym lokalnie oprogramowaniem IBM Security Access Management (ISAM) dołączonym do niej jako oprogramowanie pomocnicze. W ten sposób powstało rozwiązanie, które umożliwia pionom przedsiębiorstw Klientów zarządzanie dostępem do aplikacji zarówno zainstalowanych lokalnie, jak i działających w chmurze.

1.1.3 IBM Cloud Identity Connect for ISAM

Ta Usługa Przetwarzania w Chmurze jest ściśle zintegrowana z zainstalowanym lokalnie oprogramowaniem IBM Security Access Management (ISAM). W ten sposób powstało rozwiązanie, które umożliwia pionom przedsiębiorstw Klientów zarządzanie dostępem do aplikacji zarówno zainstalowanych lokalnie, jak i działających w chmurze. W przypadku niniejszej Usługi Przetwarzania w Chmurze Klient musi mieć aktywne uprawnienie do Subskrypcji i Wsparcia Oprogramowania dla programu IBM Security Access Management (ISAM), przy czym ta usługa Subskrypcji i Wsparcia musi pozostać aktywna przez cały czas obowiązywania subskrypcji Klienta na Usługę Przetwarzania w Chmurze. Uprawnienia Klienta do tej Usługi Przetwarzania w Chmurze muszą odpowiadać uprawnieniom licencyjnym Klienta do oprogramowania ISAM w środowisku lokalnym. Deaktywacja używanej przez Klienta usługi Subskrypcji i Wsparcia powoduje również deaktywację niniejszej Usługi Przetwarzania w Chmurze. Niniejsza Usługa Przetwarzania w Chmurze nie obejmuje dostępu do oprogramowania pomocniczego wskazanego w paragrafie 5.2.

1.1.4 IBM Cloud Identity Essentials

W ramach tej Usługi Przetwarzania w Chmurze dostępne są funkcje pojedynczego logowania (SSO) do różnych aplikacji IBM oraz aplikacji działających w chmurze publicznej, z których korzysta Klient. Usługę tę można połączyć z usługą IBM MaaS360 w celu zapewnienia dodatkowych poziomów kontroli bezpieczeństwa, na przykład dostępu warunkowego.

1.1.5 IBM Cloud Identity Verify

W ramach tej Usługi Przetwarzania w Chmurze dostępne są funkcje uwierzytelniania wieloskładnikowego w aplikacjach chronionych przez usługę Cloud Identity Connect oraz za pośrednictwem bezpośredniego wywołania funkcji API. Obsługiwane są również inne punkty kontroli dostępu, m.in. klienty RADIUS,

serwery PAM z systemem Unix/Linux i serwery Windows, w celu weryfikacji tożsamości podczas uzyskiwania dostępu do usług cyfrowych. Obejmuje to takie mechanizmy jak hasła jednorazowe przesyłane pocztą elektroniczną i w wiadomości SMS oraz hasła o ograniczonym czasie ważności (znaczniki programowe), a także uwierzytelnianie biometryczne oparte na technologii push obsługiwane przez rozwiązanie IBM Verify. Ta Usługa Przetwarzania w Chmurze jest zintegrowana z zainstalowanym lokalnie oprogramowaniem IBM Security Access Management (ISAM). W ten sposób powstało rozwiązanie, które umożliwia pionom przedsiębiorstw Klientów zarządzanie dostępem do aplikacji zarówno zainstalowanych lokalnie, jak i działających w chmurze. Jest ono dostępne w wersji autonomicznej oraz jako uzupełnienie usług Cloud Identity Connect, Cloud Identity Connect for ISAM i Cloud Identity Essentials.

1.1.6 IBM Cloud Identity Govern

Ta Usługa Przetwarzania w Chmurze jest ściśle zintegrowana z zainstalowanym lokalnie oprogramowaniem IBM Security Identity Governance and Intelligence (IGI) i IBM Security Identity Manager (ISIM) dołączonym do niej jako oprogramowanie pomocnicze. W ten sposób powstało rozwiązanie, które umożliwia pionom przedsiębiorstw Klientów zarządzanie dostępem do aplikacji zarówno zainstalowanych lokalnie, jak i działających w chmurze. Ta Usługa Przetwarzania w Chmurze udostępnia organizacjom zaawansowane możliwości zarządzania cyklem życia tożsamości użytkowników w środowisku chmury. Obejmuje przepływ pracy dotyczący żądań dostępu do aplikacji.

1.1.7 IBM Cloud Identity Connect and Verify

Ta Usługa Przetwarzania w Chmurze zapewnia Klientowi dostęp do funkcji usług IBM Cloud Identity Connect i IBM Cloud Identity Verify w ramach jednego produktu oferowanego.

1.1.8 IBM Cloud Identity Analyze

Ta Usługa Przetwarzania w Chmurze wzbogaca istniejące rozwiązania IBM, takie jak IBM Security Identity Governance and Intelligence (IGI) i IBM Security Identity Manager (ISIM), co pozwala określić kompleksowy profil ryzyka dla zarządzanych użytkowników. Usługa udostępnia lokalny, wielofunkcyjny mechanizm analityczny, który przetwarza dane dotyczące działań i uprawnień pochodzące z różnych źródeł. Zapewnia to pełny obraz czynników ryzyka związanych z dostępem i daje możliwość podjęcia działań na podstawie uzyskanych informacji.

1.1.9 IBM Cloud Identity Adaptive Access

Ta Usługa Przetwarzania w Chmurze wykorzystuje uzyskane za pomocą funkcji sztucznej inteligencji kontekstowe informacje na temat użytkowników oraz ich urządzeń i wzorców zachowania, aby ułatwić przedsiębiorstwom egzekwowanie właściwych reguł uwierzytelniania.

1.1.10 IBM Cloud Identity Connect Verify and Govern

Ta Usługa Przetwarzania w Chmurze zapewnia Klientowi dostęp do funkcji usług IBM Cloud Identity Connect, IBM Cloud Identity Verify i IBM Cloud Identity Govern w ramach jednego produktu oferowanego.

1.2 Usługi Opcjonalne

1.2.1 IBM Security Verify Non-Production

Usługa IBM Security Verify Non-Production Environment on Cloud to odrębna instancja platformy IBM Security Verify, która może być używana wyłącznie w wewnętrznej działalności pozaprodukcyjnej Klienta, a w szczególności do testowania, dostrajania wydajności, diagnozowania błędów, wykonywania wewnętrznych testów porównawczych, przemieszczania danych, zapewniania jakości i/lub programowania dodatków lub rozszerzeń do Usługi Przetwarzania w Chmurze do użytku wewnętrznego za pomocą opublikowanych aplikacyjnych interfejsów programistycznych. Do niniejszej Usługi Przetwarzania w Chmurze może zostać opcjonalnie włączona umowa dotycząca poziomu usług w zakresie dostępności, z zastrzeżeniem warunków określonych w paragrafie 3 „Poziomy Usług i wsparcie techniczne”. W ramach tej Usługi Przetwarzania w Chmurze możliwe jest przetwarzanie 100 Zdarzeń na sekundę.

1.2.2 IBM Security Verify Vanity Domain

Opcja domeny indywidualnej (ang. vanity domain) umożliwia Klientowi używanie domeny, która należy do jego przedsiębiorstwa i jest lepiej do niego dostosowana, zamiast domyślnej domeny użytkownika udostępnianej standardowo na platformie. IBM będzie utrzymywać dla tej domeny certyfikat SSL odnawiany raz w roku.

1.2.3 IBM Security Verify Application Gateway Hosted

Brama aplikacji to zarządzane i udostępniane przez IBM uproszczone urządzenie przeznaczone dla Klientów, którzy chcą obsługiwać niestandardowe lub wcześniej stosowane mechanizmy uwierzytelniania. Do takich mechanizmów należą między innymi uwierzytelnianie oparte na protokole LTPA i sprawdzaniu nagłówka HTTP. Działania związane z bieżącym monitorowaniem i serwisowaniem są zarządzane przez IBM.

1.2.4 IBM Security Verify SMS and Email One-time Password

W ramach tej usługi udostępniane są hasła jednorazowe przesyłane pocztą elektroniczną i w wiadomości SMS jako drugi składnik mechanizmu uwierzytelniania.

1.2.5 IBM Security Verify Account Synchronization

Synchronizacja kont to proces, za pośrednictwem którego konta z aplikacji docelowych skonfigurowane na potrzeby udostępniania są pobierane i wprowadzane do usługi Security Verify. Proces ten obejmuje przeprowadzanie weryfikacji opartej na istniejących danych kont oraz stosowanie strategii wdrażania i wykonywania działań naprawczych w celu utrzymania systemu w stanie spójnym z aplikacją docelową.

1.2.6 IBM Cloud Identity Non-Production

Usługa IBM Cloud Identity Non-Production Environment on Cloud to odrębna instancja platformy IBM Cloud Identity, która może być używana wyłącznie w wewnętrznej działalności pozaprodukcyjnej Klienta, a w szczególności do testowania, dostrajania wydajności, diagnozowania błędów, wykonywania wewnętrznych testów porównawczych, przemieszczania danych, zapewniania jakości i/lub programowania dodatków lub rozszerzeń do Usługi Przetwarzania w Chmurze do użytku wewnętrznego za pomocą opublikowanych aplikacyjnych interfejsów programistycznych. Do niniejszej Usługi Przetwarzania w Chmurze może zostać opcjonalnie włączona umowa dotycząca poziomu usług w zakresie dostępności, z zastrzeżeniem warunków określonych w paragrafie 3 „Poziomy Usług i wsparcie techniczne”. W ramach tej Usługi Przetwarzania w Chmurze możliwe jest przetwarzanie 100 Zdarzeń na sekundę.

1.2.7 IBM Cloud Identity Vanity Domain

Opcja domeny indywidualnej (ang. vanity domain) umożliwia Klientowi używanie domeny, która należy do jego przedsiębiorstwa i jest lepiej do niego dostosowana, zamiast domyślnej domeny użytkownika udostępnianej standardowo na platformie. IBM będzie utrzymywać dla tej domeny certyfikat SSL odnawiany raz w roku.

1.2.8 IBM Cloud Identity Application Gateway Hosted

Brama aplikacji to zarządzane i udostępniane przez IBM uproszczone urządzenie przeznaczone dla Klientów, którzy chcą obsługiwać niestandardowe lub wcześniej stosowane mechanizmy uwierzytelniania. Do takich mechanizmów należą między innymi uwierzytelnianie oparte na protokole LTPA i sprawdzaniu nagłówka HTTP. Działania związane z bieżącym monitorowaniem i serwisowaniem są zarządzane przez IBM.

1.3 Usługi przyspieszające

1.3.1 IBM Security Verify Solution Planning

Ta oferta obejmuje 1 (jeden) tydzień usług specjalistycznych, w czasie którego IBM wykona niektóre lub wszystkie spośród wymienionych poniżej zadań:

- Utworzenie mechanizmu pojedynczego logowania dla aplikacji SaaS działających w chmurze.
- Skonfigurowanie punktu wyjścia ułatwiającego lokalizowanie aplikacji.
- Połączenie aplikacji z gotowymi konektorami.
- Planowanie rozwiązań, opracowanie architektury i udzielanie wskazówek.
- Przedstawienie zalecanego przez IBM podejścia i procedur.

1.3.2 IBM Security Verify Workshop for Multi-Factor Authentication

W ramach tej oferty organizowane są trzydniowe warsztaty w zakresie usług specjalistycznych, dotyczące przede wszystkim uwierzytelniania wieloskładnikowego oraz ochrony aplikacji Klienta za pomocą rozwiązania IBM Cloud Identify Verify. Tematy tych warsztatów obejmują:

- Wbudowywanie znanych mechanizmów uwierzytelniania we wszystkie interakcje osobiste i cyfrowe, w przypadku których wymagane jest uwierzytelnianie.
- Stosowanie silnego uwierzytelniania w aplikacjach z wykorzystaniem przyjaznego dla programistów interfejsu API w architekturze REST.
- Udostępnianie zaleceń i sprawdzonych procedur branżowych dotyczących bezpieczeństwa tożsamości.
- Dostosowanie i uproszczenie interfejsu użytkownika na wszystkich urządzeniach – telefonach, tabletach i laptopach.

1.3.3 IBM Security Verify Strategy and Planning

W ramach tej usługi organizowane są trzytygodniowe warsztaty w zakresie usług specjalistycznych, dotyczące wykorzystywania sprawdzonych procedur z zakresu bezpieczeństwa w chmurze, ze szczególnym uwzględnieniem bezpieczeństwa infrastruktur i aplikacji. Tematy tych warsztatów obejmują:

- Utworzenie mechanizmu pojedynczego logowania dla aplikacji SaaS działających w chmurze.
- Skonfigurowanie punktu wyjścia ułatwiającego lokalizowanie aplikacji.
- Połączenie aplikacji z gotowymi konektorami.
- Planowanie rozwiązań, opracowanie architektury i udzielanie wskazówek.
- Udostępnianie informacji dotyczących nowych trendów w dziedzinie cyberbezpieczeństwa.
- Przedstawienie zalecanego przez IBM podejścia i procedur.

1.3.4 IBM Security Verify Expert On Demand

Oferta ta obejmuje 20 (dwadzieścia) godzin usług specjalistycznych świadczonych w ramach dwugodzinnych sesji, które odbędą się w ciągu 30 (trzydziestu) dni od daty rozpoczęcia. W ramach tych sesji architekt ds. usług IBM Security Verify odpowie na pytania oraz udzieli porad i zaleceń w następującym zakresie:

- Wiedza techniczna umożliwiająca efektywniejszą implementację rozwiązania Klienta.
- Architektura i implementacja rozwiązania Klienta.
- Wskazówki dotyczące rozwiązania i/lub strategii Klienta.

1.3.5 IBM Cloud Identity Connect Solution Planning

Ta oferta obejmuje 1 (jeden) tydzień usług specjalistycznych, w czasie którego IBM wykona niektóre lub wszystkie spośród wymienionych poniżej zadań:

- Utworzenie mechanizmu pojedynczego logowania dla aplikacji SaaS działających w chmurze.
- Skonfigurowanie punktu wyjścia ułatwiającego lokalizowanie aplikacji.
- Połączenie aplikacji z gotowymi konektorami.
- Planowanie rozwiązań, opracowanie architektury i udzielanie wskazówek.
- Przedstawienie zalecanego przez IBM podejścia i procedur.

1.3.6 IBM Cloud Identity Verify Workshop for Multi-Factor Authentication

W ramach tej oferty organizowane są trzydniowe warsztaty w zakresie usług specjalistycznych, dotyczące przede wszystkim uwierzytelniania wieloskładnikowego oraz ochrony aplikacji Klienta za pomocą rozwiązania IBM Cloud Identify Verify. Tematy tych warsztatów obejmują:

- Wbudowywanie znanych mechanizmów uwierzytelniania we wszystkie interakcje osobiste i cyfrowe, w przypadku których wymagane jest uwierzytelnianie.
- Stosowanie silnego uwierzytelniania w aplikacjach z wykorzystaniem przyjaznego dla programistów interfejsu API w architekturze REST.
- Udostępnianie zaleceń i sprawdzonych procedur branżowych dotyczących bezpieczeństwa tożsamości.
- Dostosowanie i uproszczenie interfejsu użytkownika na wszystkich urządzeniach – telefonach, tabletach i laptopach.

1.3.7 IBM Cloud Security Strategy and Planning

W ramach tej usługi organizowane są trzytygodniowe warsztaty w zakresie usług specjalistycznych, dotyczące wykorzystywania sprawdzonych procedur z zakresu bezpieczeństwa w chmurze, ze szczególnym uwzględnieniem bezpieczeństwa infrastruktur i aplikacji. Tematy tych warsztatów obejmują:

- Utworzenie mechanizmu pojedynczego logowania dla aplikacji SaaS działających w chmurze.
- Skonfigurowanie punktu wyjścia ułatwiającego lokalizowanie aplikacji.
- Połączenie aplikacji z gotowymi konektorami.
- Planowanie rozwiązań, opracowanie architektury i udzielanie wskazówek.
- Udostępnianie informacji dotyczących nowych trendów w dziedzinie cyberbezpieczeństwa.
- Przedstawienie zalecanego przez IBM podejścia i procedur.

1.3.8 IBM Cloud Identity Expert On Demand

Oferta ta obejmuje 20 (dwadzieścia) godzin usług specjalistycznych świadczonych w ramach dwugodzinnych sesji, które odbędą się w ciągu 30 (trzydziestu) dni od daty rozpoczęcia. W ramach tych sesji architekt ds. usług Cloud Identity odpowie na pytania oraz udzieli porad i zaleceń w następującym zakresie:

- Wiedza techniczna umożliwiająca efektywniejszą implementację rozwiązania Cloud Identity Klienta.
- Architektura i implementacja rozwiązania Cloud Identity Klienta.
- Wskazówki dotyczące rozwiązania Cloud Identity Klienta i/lub związanej z nim strategii.

2. Specyfikacje techniczne dotyczące przetwarzania i ochrony danych

Dodatek IBM dotyczący Przetwarzania Danych dostępny pod adresem http://ibm.com/dpa (dalej „DPD”) oraz Specyfikacja Techniczna dotycząca Przetwarzania i Ochrony Danych (dalej „Specyfikacja Techniczna” lub „Załącznik Szczegółowy do DPD”) dostępna za pośrednictwem zamieszczonych poniżej odsyłaczy zawierają dodatkowe informacje na temat ochrony danych dla Usług Przetwarzania w Chmurze oraz ich opcji. Informacje te precyzują, jakie rodzaje Zawartości mogą być przetwarzane przez daną Usługę, jakie czynności przetwarzania są realizowane, jakie są opcje ochrony danych, a także jakie są szczegółowe zasady przechowywania i zwrotu Zawartości. Jeśli do Zawartości stosuje się i) ogólne rozporządzenie o ochronie danych (RODO – UE/2016/679) lub ii) inne regulacje dotyczące ochrony danych osobowych określone pod adresem http://ibm.com/dpa/dpl, to w zakresie, w jakim przepisy te mają zastosowanie do danych osobowych uwzględnionych w Zawartości, obowiązuje DPD.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D

3. Poziomy Usług i wsparcie techniczne

3.1 Umowa dotycząca Poziomu Usług

IBM udostępnia Klientowi przedstawioną poniżej Umowę dotyczącą Poziomu Usług („SLA”). IBM naliczy najwyższe obowiązujące wyrównanie na podstawie łącznej dostępności Usługi Przetwarzania w Chmurze, zgodnie z poniższą tabelą. Dostępność wyrażona procentowo jest równa ilorazowi łącznej liczby minut w danym miesiącu obowiązywania umowy, pomniejszonej o łączną liczbę minut Wyłączenia Usługi w tym miesiącu, oraz łącznej liczby minut w tym miesiącu. Jest ona powiązana z danym regionem oraz liczbą użytkowników objętych subskrypcją w tym regionie. Definicja Wyłączenia Usługi, opis procesu zgłaszania reklamacji oraz informacje o sposobie kontaktowania się z IBM w sprawach związanych z dostępnością usług znajdują się w Przeglądzie wsparcia technicznego dla usług IBM SaaS pod adresem https://www.ibm.com/software/support/saas_support_overview.html.

Dostępność	Uznanie (% miesięcznej opłaty za subskrypcję*)
Poniżej 99,9%	10%

* Opłata za subskrypcję oznacza cenę w miesiącu obowiązywania umowy, którego dotyczy reklamacja.

3.1.1 Inne informacje na temat niniejszej Umowy dotyczącej Poziomu Usług

W ciągu pierwszych 60 (sześćdziesięciu) dni Okresu Obowiązywania („Okres Docierania”) Klientowi nie przysługuje żadne uznanie, jeśli w ramach niniejszej Umowy wyrażony procentowo czas dostępności środowiska Usługi Przetwarzania w Chmurze nie osiągnie minimalnego poziomu 99,9%. Jeśli przed Okresem Docierania lub w jego trakcie IBM zidentyfikuje istniejące konfiguracje, strategie, dane lub kod Klienta („Wcześniej Istniejące Komponenty”) przeznaczone do migracji do Usługi Przetwarzania w Chmurze, które uniemożliwiają pomyślne osiągnięcie wyrażonego procentowo czasu dostępności Usługi Przetwarzania w Chmurze w ramach niniejszej Umowy, wówczas IBM zastrzega sobie prawo do powiadomienia Klienta o takich Wcześniej Istniejących Komponentach oraz do wyłączenia ich według własnego uznania z zakresu postanowień umowy dotyczącej poziomu usług. Jeśli IBM powiadomi Klienta o Wcześniej Istniejących Komponentach wyłączonych z zakresu postanowień umowy dotyczącej poziomu usług, IBM ma obowiązek przedstawić Klientowi plan możliwego zakresu działań zaradczych, który umożliwi takim komponentom osiągnięcie określonego w niniejszej Umowie wyrażonego procentowo czasu dostępności. O ile Strony nie uzgodnią inaczej, Klient ponosi wyłączną odpowiedzialność za koszt takich działań zaradczych.

3.2 Wsparcie techniczne

Informacje o wsparciu technicznym dla Usługi Przetwarzania w Chmurze, w tym dane kontaktowe, poziomy istotności, godziny świadczenia usług, czasy reakcji oraz inne informacje i procesy, można znaleźć w podręczniku wsparcia IBM, dostępnym pod adresem https://www.ibm.com/support/home/pages/support-guide/ (należy wybrać odpowiednią Usługę Przetwarzania w Chmurze).

4. Opłaty

4.1 Opłaty rozliczeniowe

Opłaty rozliczeniowe za Usługę Przetwarzania w Chmurze są określone w Dokumencie Transakcyjnym.

Przy sprzedaży niniejszej Usługi Przetwarzania w Chmurze wysokość opłat rozliczeniowych jest ustalana na podstawie jednej z następujących miar:

- Instancja to każdy dostęp do konkretnej konfiguracji Usługi Przetwarzania w Chmurze.
- Przedsięwzięcie to usługa specjalistyczna lub szkoleniowa związana z Usługami Przetwarzania w Chmurze.
- Zdarzenie to wystąpienie określonego zdarzenia, które jest przetwarzane przez Usługi Przetwarzania w Chmurze lub związane z ich używaniem.
    - W usłudze Security Verify SMS and One-Time Password Zdarzeniem jest wysłanie jednorazowego hasła w wiadomości e-mail lub SMS.
    - W usłudze Cloud Identity Connect Zdarzeniem jest żądanie HTTP przesłane do Usługi Przetwarzania w Chmurze.
    - W usłudze Cloud Identity Verify Zdarzeniem jest wywołanie dowolnej metody wieloskładnikowej za pośrednictwem Usługi Przetwarzania w Chmurze.
- Autoryzowany Użytkownik to unikalny użytkownik, który ma prawo dostępu do Usługi Przetwarzania w Chmurze w jakikolwiek sposób, bezpośrednio lub pośrednio (na przykład przez program multipleksujący, urządzenie lub serwer aplikacji), przy użyciu dowolnych środków.
- Pracownik to unikalna osoba zatrudniona w Przedsiębiorstwie Klienta, opłacana przez nie lub działająca w jego imieniu (niezależnie od tego, czy został jej przyznany dostęp do Usług Przetwarzania w Chmurze).
- Uprawniony Uczestnik to osoba lub podmiot uprawniony do uczestnictwa w dowolnym programie świadczenia usługi zarządzanym lub monitorowanym za pomocą Usług Przetwarzania w Chmurze.
- Jednostka Zasobów to niezależna miara zasobów, które są przetwarzane lub zarządzane przez Usługę Przetwarzania w Chmurze bądź związane z jej używaniem.

  Użycie każdej możliwości funkcjonalnej wymaga nabycia określonej liczby uprawnień opartych na Jednostkach Zasobów w ramach subskrypcji niniejszej Usługi Przetwarzania w Chmurze:

		Możliwość funkcjonalna określona w ważonych Jednostkach Zasobów wymaganych dla każdego Użytkownika				
Warstwa stopniowana	**Maksymalna liczba aktywnych użytkowników miesięcznie**	**Pojedyncze logowanie**	**Uwierzytelnianie wieloskładnikowe**	**Dostęp adaptacyjny**	**Zarządzanie cyklem życia i nadzór**	**Analiza**
1	500	0,1000	0,1000	0,1000	0,2900	0,1200
2	5000	0,0800	0,0090	0,0090	0,0750	0,1000
3	10 000	0,0600	0,0080	0,0080	0,0500	0,0750
4	100 000	0,0080	0,0060	0,0060	0,0050	0,0200
5	500 000	0,0020	0,0020	0,0020	0,0020	0,0150
6	1 000 000	0,0015	0,0010	0,0010	0,0010	0,0010
7	5 000 000	0,0010	0,0005	0,0005	0,0005	0,0005
8	10 000 000	0,0005	0,0004	0,0004	0,0002	0,0002
9	50 000 000	0,0002	0,0002	0,0002	0,0001	0,0001
10	999 999 999	0,0001	0,0001	0,0001	0,0001	0,0001

5. Warunki dodatkowe

Dla Umów o Usługi Przetwarzania w Chmurze (lub podstawowych umów o usługi przetwarzania w chmurze będących ich odpowiednikami) zawartych przed 1 stycznia 2019 r. mają zastosowanie warunki zamieszczone pod adresem https://www.ibm.com/acs.

5.1 Odniesienia do Klienta

Klient wyraża zgodę na publikowanie przez IBM w komunikatach reklamowych lub marketingowych informacji o Kliencie jako subskrybencie Usług Przetwarzania w Chmurze.

5.2 Oprogramowanie pomocnicze

Usługa Przetwarzania w Chmurze zawiera następujące oprogramowanie pomocnicze:

- IBM Security Verify Bridge
- IBM Security Verify
- IBM Security Verify SDK (iOS)
- IBM Security Verify SDK (Android)
- IBM Security Verify SDK for JavaScript
- IBM Security Verify Bridge for Directory Sync
- IBM Application Gateway
- IBM Security Verify Hosted Application Gateway
- IBM Security Verify Gateway for Windows Login
- IBM Security Verify Gateway for PAM (on AIX)
- IBM Security Verify Gateway for PAM
- IBM Security Verify Gateway for RADIUS
- IBM Security Verify Credentials

Następujące oprogramowanie pomocnicze może być używane wyłącznie z Usługami Przetwarzania w Chmurze IBM Cloud Identity Connect, IBM Cloud Identity Connect and Verify oraz IBM Cloud Identity Connect Verify and Govern:

- IBM Security Access Manager Virtual Enterprise Edition

Następujące oprogramowanie pomocnicze może być używane wyłącznie z Usługami Przetwarzania w Chmurze IBM Security Verify, IBM Cloud Identity Govern oraz IBM Cloud Identity Connect Verify and Govern:

- IBM Security Identity Governance and Intelligence Enterprise Edition
- IBM Security Identity Manager