Rublon

Uwierzytelnianie wieloskładnikowe: Przewodnik zakupowy

Spis treści

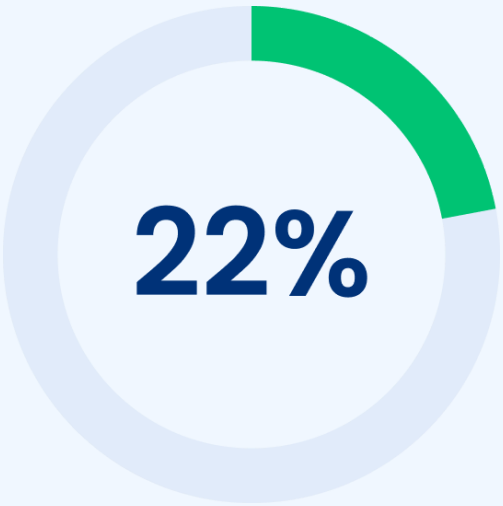
1. Wstęp **3**
1.1. Dlaczego wybór odpowiedniego rozwiązania MFA ma znaczenie? 3
1.2. Jak korzystać z tego poradnika? 4
2. Zdefiniuj, czego potrzebuje organizacja **6**
2.1. Zacznij od wymagań biznesowych i bezpieczeństwa 6
2.2. Identyfikacja użytkowników, aplikacji i ścieżek dostępu 9
2.3. Unikanie częściowego zakresu ochrony MFA 10
3. Ocena skuteczności zabezpieczeń **11**
3.1. Ocena siły metod uwierzytelniania 11
3.2. Priorytetowe traktowanie MFA odpornego na phishing 13
3.3. Ocena ochrony przed atakiem typu MFA fatigue i socjotechniką 14
3.4. Analiza polityk dostępu i ich egzekwowania 15
3.5. Weryfikacja możliwości rejestrowania, monitorowania i reagowania na incydenty 17
4. Ocena zakresu ochrony infrastruktury i integracji **18**
4.1. Ochrona środowisk chmurowych, lokalnych i hybrydowych 18
4.2. Ocena zakresu integracji 20
4.3. Sprawdzenie zgodności protokołów i źródeł tożsamości 21
4.4. Ocena obsługi aplikacji niestandardowych i aplikacji typu legacy 23
5. Ocena doświadczenia użytkowników i administratorów **24**
5.1. Doświadczenie związane z uwierzytelnianiem 24
5.2. Rejestracja i cykl życia uwierzytelniacza 26
5.3. Doświadczenie administratorów i delegowanie uprawnień 27
6. Ocena wdrożenia i eksploatacji **28**
6.1. Architektura wdrożenia 28
6.2. Czas wdrożenia i czas do osiągnięcia ochrony 29
6.3. Dostępność, odporność i odzyskiwanie 31
6.4. Wymagania dotyczące utrzymania i aktualizacji 32
7. Ocena aspektów handlowych i dostawcy **33**
7.1. Obliczanie całkowitego kosztu posiadania 33
7.2. Zapewnienie bezpieczeństwa, prywatność i zgodność 35
7.3. Ocena nie tylko produktu, ale i dostawcy 36
8. Przeprowadzenie miarodajnej weryfikacji koncepcji **37**
8.1. Opracowanie planu weryfikacji koncepcji rozwiązania MFA 37
8.1.1. Określenie kryteriów powodzenia 37
8.1.2. Zastosowanie reprezentatywnych scenariuszy 38
8.1.3. Gromadzenie dowodów 38

8.2. Karta oceny dostawcy rozwiązania MFA 39
8.3. Arkusz oceny dostawcy 40
8.4. Sygnały ostrzegawcze podczas oceny dostawcy MFA 41
9. Jak rozwiązanie Rublon MFA spełnia kryteria oceny? 41
9.1. Najważniejsze informacje o rozwiązaniu Rublon MFA 41
9.2. Ochrona krytycznych ścieżek dostępu w organizacji 42
9.3. Metody uwierzytelniania dla różnych użytkowników i poziomów ryzyka 44
9.4. Scentralizowane polityki, administracja i widoczność 45
9.5. Wdrożenie w istniejącej infrastrukturze 46
9.6. Korzyści operacyjne i kwestie dotyczące całkowitego kosztu 47
9.7. Pomoc techniczna, dokumentacja i zapewnienie bezpieczeństwa 48
10. Podsumowanie i materiały dla kupujących 48
10.1. Końcowa lista kontrolna dla kupującego rozwiązanie MFA 48
10.1.1. Zakres i ochrona 48
10.1.2. Uwierzytelnianie i polityki 49
10.1.3. Eksploatacja i odporność 49
10.1.4. Ocena warunków handlowych i dostawcy 50
10.1.5. Gotowość do wdrożenia 50
10.2. Następne kroki 50

1. Wstęp

1.1. Dlaczego wybór odpowiedniego rozwiązania MFA ma znaczenie?

Wdrożenie rozwiązania do uwierzytelniania wieloskładnikowego (MFA) nie zapewnia automatycznie skutecznej ochrony całej organizacji. Poziom bezpieczeństwa zależy od tego, które ścieżki dostępu są chronione, jakie metody są dozwolone, w jaki sposób egzekwowane są polityki oraz jak platforma obsługuje odzyskiwanie dostępu, wyjątki i awarie infrastruktury.



Dlaczego uwierzytelnianie MFA jest ważne?

Kradzież danych uwierzytelniających nadal stanowi powszechną metodę uzyskiwania dostępu do systemów firmowych. Atakujący zdobywają hasła za pomocą ataków phishingowych, złośliwego oprogramowania typu infostealer, ataków typu credential stuffing, socjotechniki oraz wykorzystywania tych samych haseł w wielu usługach. Przejęte dane uwierzytelniające stanowiły początkowy wektor dostępu w **22%** naruszeń przeanalizowanych w raporcie Verizon 2025 Data Breach Investigations Report. Badania firmy Verizon pokazują również, że nadużycia związane z danymi uwierzytelniającymi mogą stanowić znaczną część codziennego ruchu uwierzytelniającego.

Atakujący coraz częściej obierają za cel sam proces uwierzytelniania. Atak phishingowy typu adversary-in-the-middle może przekazywać hasła i jednorazowe kody dostępu do prawidłowej usługi. Atak typu push bombing ma na celu wywarcie presji na użytkownikach, aby zatwierdzili fałszywe żądania. Skradzione tokeny sesji mogą umożliwić atakującym ponowne wykorzystanie

© 2026 Rublon

uwierzytelnionej sesji bez konieczności ponownego przechodzenia procesu uwierzytelniania MFA.

Amerykański Narodowy Instytut Standaryzacji i Technologii (NIST) nie klasyfikuje ręcznie wprowadzanych kodów jednorazowych jako metod odpornych na phishing, ponieważ kody te mogą zostać przechwycone i przekazane dalej. Amerykańska Agencja ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA) zaleca przechodzenie, tam gdzie jest to możliwe, na uwierzytelnianie oparte na standardach FIDO i WebAuthn.

Proste wdrożenie rozwiązania MFA może spełnić ograniczone wymagania audytowe, ale jednocześnie pozostawić istotne luki w zabezpieczeniach. Ochroną mogą zostać objęte aplikacje chmurowe, podczas gdy sieci VPN, uprzywilejowane logowania do systemu Windows, serwery z systemem Linux lub systemy typu legacy nadal będą wymagać wyłącznie hasła. Nieskuteczne procedury odzyskiwania dostępu i niewłaściwie kontrolowana rejestracja uwierzytelniaczy mogą dodatkowo osłabić skuteczność uwierzytelniania, które w innych warunkach zapewniałoby wysoki poziom bezpieczeństwa.

Nieodpowiednia platforma MFA generuje również koszty operacyjne. Skomplikowany proces rejestracji zwiększa liczbę zgłoszeń do działu pomocy technicznej. Ograniczona obsługa integracji prowadzi do korzystania z równoległych narzędzi. Niewłaściwie dobrane metody powodują opór użytkowników i stosowanie sposobów obchodzenia zabezpieczeń. Koszty sprzętu, usług telefonicznych, usług profesjonalnych, infrastruktury, utrzymania i pracy wewnętrznych zespołów mogą z czasem sprawić, że pozornie niedrogi produkt stanie się kosztowny.

Odpowiednie rozwiązanie musi zapewniać równowagę między bezpieczeństwem, zakresem ochrony, łatwością użytkowania, nakładem pracy związanym z wdrożeniem, odpornością na awarie i kosztami. Jego celem nie jest jedynie dodanie kolejnego monitu, lecz ograniczenie ryzyka przejęcia kont bez tworzenia nowych luk w zabezpieczeniach i zbędnych utrudnień.

1.2. Jak korzystać z tego poradnika?

Każda decyzja dotycząca rozwiązania MFA wpływa na architekturę bezpieczeństwa, działanie infrastruktury, zgodność z przepisami, produktywność użytkowników, obciążenie działu pomocy technicznej oraz długoterminowe koszty. Poszczególni interesariusze powinni oceniać tę samą platformę z własnej perspektywy operacyjnej:

© 2026 Rublon

- Dyrektorzy ds. bezpieczeństwa informacji (CISO) i osoby odpowiedzialne za bezpieczeństwo mogą ocenić stopień ograniczenia ryzyka związanego z tożsamością.
- Dyrektorzy IT, administratorzy infrastruktury i zespoły sieciowe mogą skoncentrować się na integracji, wdrożeniu, odporności na awarie i utrzymaniu.
- Zespoły ds. zarządzania tożsamością i dostępem (IAM) mogą analizować źródła tożsamości, metody, polityki oraz zarządzanie cyklem życia uwierzytelniaczy.
- Zespoły ds. zgodności i ryzyka powinny przeanalizować możliwości audytowe, ochronę danych oraz wsparcie w spełnianiu wymagań regulacyjnych.
- Zespoły ds. zakupów mogą porównać modele licencjonowania, koszty wdrożenia, warunki pomocy technicznej i dodatkowe opłaty.
- Dostawcy usług zarządzanych powinni również uwzględnić skalowalność, delegowane zarządzanie i separację dzierżawców.

Ocena obejmuje osiem powiązanych obszarów:

- Skuteczność zabezpieczeń
- Metody uwierzytelniania
- Zakres integracji i ochrony infrastruktury
- Polityki dostępu i zarządzanie
- Doświadczenie użytkownika
- Wdrożenie i eksploatacja
- Niezawodność i wiarygodność dostawcy
- Całkowity koszt posiadania

Podczas oceny należy wziąć pod uwagę wszystkie te obszary. Silne uwierzytelnianie ma ograniczoną wartość, jeżeli ważne systemy pozostają bez ochrony. Szeroki zakres integracji jest mniej atrakcyjny, jeżeli zarządzanie staje się rozproszone lub użytkownicy nie mogą niezawodnie ukończyć procesu uwierzytelniania.

© 2026 Rublon



Rzetelna ocena MFA wymaga spojrzenia na osiem powiązanych obszarów, a nie tylko na dostępne metody uwierzytelniania.

2. Zdefiniuj, czego potrzebuje organizacja

2.1. Zacznij od wymagań biznesowych i bezpieczeństwa

Zacznij nie od listy funkcji oferowanych przez dostawcę, tylko od problemu, który organizacja musi rozwiązać.

Głównym celem może być ograniczenie ryzyka przejęcia kont, spełnienie wymagań regulacyjnych lub warunków ubezpieczenia cybernetycznego, realizacja umowy z klientem albo usunięcie nieprawidłowości wykrytych podczas oceny bezpieczeństwa. Czynniki operacyjne mogą obejmować pracę zdalną, uprzywilejowane działania administracyjne wykonywane z wielu lokalizacji lub kilka niekompatybilnych produktów MFA wdrożonych przez różne zespoły.

Zakres oceny należy dostosować do rzeczywistego środowiska organizacji. Aplikacje chmurowe stanowią tylko część infrastruktury. Sieci VPN, systemy Windows i Linux, urządzenia

© 2026 Rublon

sieciowe, usługi Remote Desktop Services, narzędzia administracyjne i aplikacje typu legacy mogą nadal opierać się na hasłach.

Tożsamości uprzywilejowane wymagają szczególnej uwagi. Administratorzy, pracownicy działu pomocy technicznej, zespoły odpowiedzialne za infrastrukturę i zewnętrzni dostawcy usług mogą mieć możliwość modyfikowania ustawień bezpieczeństwa, uzyskiwania dostępu do kopii zapasowych, tworzenia kont lub wyłączania mechanizmów zabezpieczeń. Należy zidentyfikować tych użytkowników, systemy, do których mają dostęp, oraz poziom siły uwierzytelniania wymagany ze względu na ich uprawnienia.

Strategia powinna również uwzględniać przyszłe zmiany. Tradycyjne metody mogą być niezbędne podczas wdrażania rozwiązania, podczas gdy klucze bezpieczeństwa zgodne ze standardem FIDO2 i klucze dostępu będą najpierw wprowadzane dla użytkowników wysokiego ryzyka, a następnie stopniowo udostępniane kolejnym grupom.

Kolejnym podstawowym wymaganiem jest widoczność. Zespoły ds. bezpieczeństwa i zgodności potrzebują wiarygodnych rejestrów prób uwierzytelnienia, decyzji wynikających z polityk, zmian dotyczących uwierzytelniaczy oraz działań administracyjnych. Platforma powinna wskazywać, kto próbował uzyskać dostęp, jakiej metody użyto oraz dlaczego dostęp został przyznany lub odrzucony.

Pisemny zestaw wymagań bazowych zapewnia zespołom ds. bezpieczeństwa, IT, zgodności i zakupów wspólną definicję sukcesu.



© 2026 Rublon

Pytania, które należy zadać:

- Które tożsamości pracowników, administratorów, kont usługowych, wykonawców, partnerów i użytkowników zewnętrznych wymagają ochrony?
- Które systemy przetwarzają dane wrażliwe, regulowane, finansowe lub krytyczne dla działalności operacyjnej?
- Które aplikacje i ścieżki dostępu nadal opierają się wyłącznie na hasłach?
- Którzy użytkownicy wymagają silniejszego uwierzytelniania?
- Których systemów nie można przenieść do nowoczesnego dostawcy tożsamości?
- Czy zakres obejmuje pracowników zdalnych, zewnętrzne zespoły pomocy technicznej oraz użytkowników bez urządzeń firmowych?
- Jakie wymagania regulacyjne, ubezpieczeniowe i kontraktowe mają zastosowanie?
- Jakie dowody muszą być dostępne na potrzeby postępowań wyjaśniających i audytów?

Arkusz wymagań dotyczących MFA

Obszar	Wymaganie	Priorytet	Stan obecny	Stan docelowy / Luki
Użytkownicy i tożsamości	Użytkownicy organizacji	**Wysoki / Średni / Niski**		
	Administratorzy i użytkownicy uprzywilejowani	**Wysoki / Średni / Niski**		
	Kontraktorzy i podmioty zewnętrzne	**Wysoki / Średni / Niski**		
	Użytkownicy zdalni	**Wysoki / Średni / Niski**		
	Konta usługowe i awaryjne	**Wysoki / Średni / Niski**		
Aplikacje i ścieżki dostępu	Aplikacje chmurowe	**Wysoki / Średni / Niski**		
	VPN i dostęp zdalny	**Wysoki / Średni / Niski**		
	Stacje robocze i serwery Windows	**Wysoki / Średni / Niski**		
	Serwery Linux i dostęp	**Wysoki / Średni /**		

© 2026 Rublon

	SSH	**Niski**		
	Dostęp do sieci i infrastruktury	**Wysoki / Średni / Niski**		
	Aplikacje legacy i niestandardowe	**Wysoki / Średni / Niski**		
Ryzyko i siła uwierzytelniania	Odporne na phishing MFA dla dostępu uprzywilejowanego	**Wysoki / Średni / Niski**		
	Silniejsze MFA dla wrażliwych aplikacji	**Wysoki / Średni / Niski**		
	Metody dla użytkowników bez smartfonów	**Wysoki / Średni / Niski**		
	Metody zapasowe i odzyskiwanie dostępu	**Wysoki / Średni / Niski**		
	Bezpieczne rejestrowanie i wymiana uwierzytelniaczy	**Wysoki / Średni / Niski**		
Zgodność i audytowalność	Wymagania regulacyjne i kontraktowe	**Wysoki / Średni / Niski**		
	Wymagania ubezpieczenia cybernetycznego	**Wysoki / Średni / Niski**		
	Rejestrowanie uwierzytelnień i działań administracyjnych	**Wysoki / Średni / Niski**		
	Retencja i eksport logów	**Wysoki / Średni / Niski**		
	Dowody wymagane podczas audytów	**Wysoki / Średni / Niski**		

2.2. Identyfikacja użytkowników, aplikacji i ścieżek dostępu

Inwentaryzacja na potrzeby MFA powinna powiązać każdy typ tożsamości z systemami, do których może uzyskać dostęp, wykorzystywaną ścieżką dostępu oraz związanym z nią

© 2026 Rublon

poziomem uprawnień. Pozwala to ujawnić niespójne mechanizmy zabezpieczeń i ścieżki dostępu oparte wyłącznie na hasłach.

Należy uwzględnić pracowników, administratorów, konta uprzywilejowane, wykonawców, partnerów i dostawców pomocy technicznej. Trzeba rejestrować zarówno dostęp lokalny, jak i zdalny. Logowanie do sieci VPN różni się od bezpośredniego dostępu do systemu Windows, natomiast usługa Remote Desktop Services może obejmować portal internetowy, bramę i hosta sesji. Administracja systemem Linux może odbywać się za pomocą protokołu SSH, a zespoły sieciowe mogą uwierzytelniać się podczas uzyskiwania dostępu do zapór sieciowych, przełączników, infrastruktury bezprzewodowej i innych urządzeń.

Aplikacje należy pogrupować według architektury i modelu integracji:

- Aplikacje chmurowe i aplikacje korzystające ze standardu SAML
- Zewnętrzne i wewnętrzne aplikacje internetowe
- Stacje robocze i serwery z systemem Windows
- Usługi Remote Desktop Services
- Serwery z systemem Linux
- Sieci VPN i urządzenia sieciowe
- Konsole administracyjne i narzędzia do zarządzania infrastrukturą
- Aplikacje niestandardowe i aplikacje typu legacy

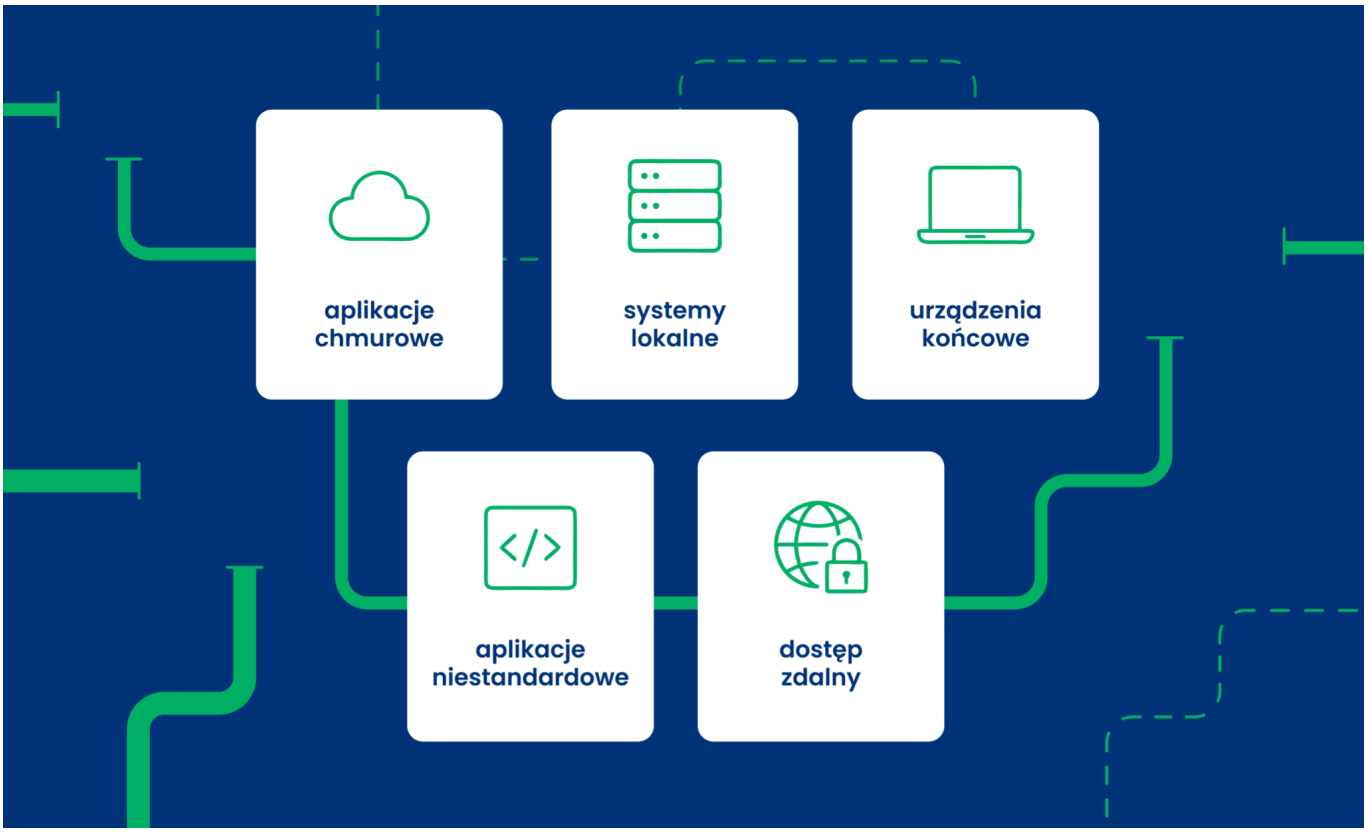
Dla każdego elementu należy zarejestrować użytkowników, źródło tożsamości, metodę logowania, lokalizację sieciową, właścicieli, poziom wrażliwości danych, poziom uprawnień oraz obecne mechanizmy uwierzytelniania. Należy również uwzględnić zależności i alternatywne punkty dostępu. Aplikacja może sprawiać wrażenie chronionej, podczas gdy jej interfejs administracyjny, konto serwisowe lub bezpośrednie logowanie do serwera nadal pozostają poza ochroną rozwiązania MFA.

2.3. Unikanie częściowego zakresu ochrony MFA

Częściowy zakres ochrony tworzy fałszywe poczucie bezpieczeństwa. Ochrona aplikacji SaaS nie zabezpiecza systemów lokalnych. Uwierzytelnianie MFA na poziomie sieci VPN nie chroni oddzielnego interfejsu zarządzania. Ochrona zdalnych logowań do systemu Windows nie zawsze oznacza automatycznie taką samą ochronę dla logowań lokalnych. Nowoczesne aplikacje mogą być objęte silnymi mechanizmami zabezpieczeń, natomiast starsze systemy zawierające równie wrażliwe dane mogą pozostać poza zakresem ochrony.

Należy prześledzić ścieżkę dostępu od użytkownika do zasobu docelowego. Każda realistyczna ścieżka prowadząca do systemu krytycznego powinna zostać zidentyfikowana i oceniona.

© 2026 Rublon



Skuteczna ochrona MFA powinna obejmować wszystkie główne strefy środowiska, nie tylko jeden obszar.

3. Ocena skuteczności zabezpieczeń

3.1. Ocena siły metod uwierzytelniania

Każdą metodę należy ocenić pod kątem potwierdzanego składnika, sposobu jego weryfikacji oraz ataków, na które dana metoda jest odporna.

Tradycyjne kategorie składników uwierzytelniania obejmują:

- **Wiedzę:** coś, co użytkownik wie, na przykład hasło lub kod PIN
- **Posiadanie:** coś, co użytkownik ma, na przykład zarejestrowany telefon lub klucz bezpieczeństwa
- **Cechy biometryczne:** właściwość biometryczna użytkownika, na przykład odcisk palca lub cecha twarzy

Dwa monity nie muszą oznaczać uwierzytelniania MFA. Dwa hasła, hasło uzupełnione pytaniem zabezpieczającym lub kody dostarczane za pośrednictwem tego samego przejętego kanału

© 2026 Rublon

mogą powodować dodatkowe utrudnienia, nie potwierdzając przy tym niezależnych składników uwierzytelniania.

Popularne metody zapewniają różne właściwości w zakresie bezpieczeństwa i działania:

- **Powiadomienie mobilne** jest szybką i dobrze znaną metodą. Jej bezpieczeństwo zwiększają dopasowywanie numerów (ang. *number matching*), informacje kontekstowe, limity żądań oraz ochrona przed powtarzającymi się monitami.
- **Kody dostępu TOTP** działają bez połączenia z siecią komórkową i są obsługiwane przez wiele aplikacji. Ponieważ użytkownicy wprowadzają je ręcznie, atakujący mogą je przechwycić i przekazać dalej.
- **Klucze bezpieczeństwa zgodne ze standardem FIDO2** wykorzystują kryptografię klucza publicznego i weryfikują prawidłową domenę usługi. Zapewniają wysoką odporność na phishing, ale wymagają procedur dystrybucji, utrzymywania zapasowych urządzeń i wymiany.
- **Klucze dostępu zgodne ze standardem FIDO2** wykorzystują kryptografię klucza publicznego i mogą być przechowywane w telefonie, komputerze, kluczu bezpieczeństwa lub w obsługiwanym module uwierzytelniania. Mogą być powiązane z urządzeniem lub synchronizowane.
- **Uwierzytelniacze platformowe**, takie jak funkcja Windows Hello, autoryzują użycie klucza dostępu za pomocą lokalnego kodu PIN, odcisku palca lub funkcji rozpoznawania twarzy.
- **Sprzętowe tokeny OTP** są odpowiednie dla użytkowników bez smartfonów oraz środowisk z ograniczoną łącznością, ale wyświetlane przez nie kody nadal mogą zostać przejęte w wyniku phishingu.
- **Metody wykorzystujące wiadomości SMS, połączenia telefoniczne i pocztę elektroniczną** zwiększają dostępność oraz mogą wspierać okres przejściowy lub odzyskiwanie dostępu. Ich bezpieczeństwo zależy od zewnętrznych kanałów komunikacji i odzyskiwania konta.
- **Uwierzytelnianie za pomocą technologii RFID** może być odpowiednie w przypadku współdzielonych stacji roboczych oraz miejsc pracy, w których już są wydawane karty pracownicze. Należy ocenić ryzyko klonowania, stosowanie kodu PIN oraz możliwość szybkiego unieważnienia dostępu.
- **Kody QR** pozwalają na wygodne skanowanie telefonem użytkownika.
- **Metody odzyskiwania dostępu**, takie jak kody pominięcia, dostęp tymczasowy i konta awaryjne, powinny być ograniczone, rejestrowane i objęte ścisłą kontrolą uprawnień.

Żadna pojedyncza metoda nie jest odpowiednia dla wszystkich użytkowników i systemów. Zrównoważony zestaw metod obejmuje uwierzytelnianie odporne na phishing dla dostępu wysokiego ryzyka, wygodne metody do codziennego użytku, alternatywy dla użytkowników bez smartfonów oraz kontrolowane metody odzyskiwania dostępu.

© 2026 Rublon

3.2. Priorytetowe traktowanie MFA odpornego na phishing

Tradycyjne uwierzytelnianie MFA może powstrzymać atakującego, który dysponuje wyłącznie skradzionym hasłem, ale nie zawsze zapewnia ochronę przed phishingiem prowadzonym w czasie rzeczywistym. Fałszywa witryna może przechwycić hasło i jednorazowy kod dostępu, a następnie przekazać oba te elementy do autentycznej usługi. Metody oparte na zatwierdzaniu żądań mogą być również nadużywane za pomocą wprowadzających w błąd lub powtarzających się monitów.

Uwierzytelnianie odporne na phishing ogranicza zależność od oceny sytuacji przez użytkownika. Amerykański Narodowy Instytut Standaryzacji i Technologii (NIST) definiuje odporność na phishing jako zdolność do zapobiegania ujawnieniu sekretów uwierzytelniających i prawidłowych danych wyjściowych uwierzytelniacza fałszywemu weryfikatorowi. Ręcznie wprowadzane jednorazowe kody dostępu czy powiadomienia push nie spełniają tej definicji.

Standard FIDO2 zapewnia odporność na phishing dzięki kryptografii klucza publicznego i standardowi WebAuthn. Podczas rejestracji uwierzytelniacz tworzy unikatowe dane uwierzytelniające dla określonej usługi. Klucz prywatny pozostaje w uwierzytelniaczu, natomiast usługa przechowuje klucz publiczny.

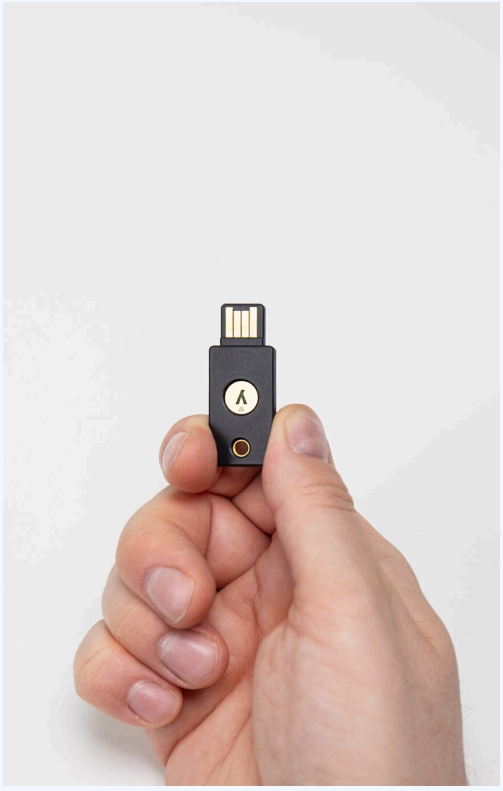
Powiązanie ze źródłem (ang. *origin binding*) zapobiega użyciu danych uwierzytelniających przez wizualnie podobną witrynę phishingową działającą w innej domenie. Przed zakończeniem uwierzytelniania uwierzytelniacz i usługa weryfikują stronę ufającą oraz źródło żądania.

Uwierzytelniacze zgodne ze standardem FIDO2 obejmują:

- **Klucze bezpieczeństwa:** oddzielne fizyczne uwierzytelniacze korzystające z USB lub NFC
- **Klucze dostępu powiązane z urządzeniem:** dane uwierzytelniające przechowywane na określonym urządzeniu lub uwierzytelniaczu
- **Synchronizowane klucze dostępu:** dane uwierzytelniające udostępniane na wielu urządzeniach za pośrednictwem chronionej usługi synchronizacji

Kod PIN lub dane biometryczne mogą służyć do lokalnej weryfikacji użytkownika. Informacje te pozostają na uwierzytelniaczu i nie są przesyłane do aplikacji jako sekret, który można ponownie wykorzystać.

© 2026 Rublon



Zalecane przypadki użycia

Uwierzytelnianie MFA odporne na phishing powinno być traktowane priorytetowo w przypadku:

- Administratorów i zespołów odpowiedzialnych za infrastrukturę
- Kont uprzywilejowanych i kont awaryjnych
- Zdalnego dostępu do systemów wewnętrznych
- Aplikacji zawierających dane podlegające regulacjom lub dane wysoce wrażliwe
- Pracowników często będących celem phishingu lub podszywania się
- Zatwierdzania operacji finansowych i autoryzacji płatności

Migrację można przeprowadzać stopniowo. Należy rozpocząć od użytkowników wysokiego ryzyka i systemów krytycznych, a następnie rozszerzać zakres w miarę zwiększania obsługi przez aplikacje i dostępności uwierzytelniaczy. Słabsze metody odzyskiwania dostępu nie mogą obniżać poziomu bezpieczeństwa zapewnianego przez silniejszą metodę podstawową.

3.3. Ocena ochrony przed atakiem typu MFA fatigue i socjotechniką

Atak typu push bombing polega na wysyłaniu powtarzających się żądań uwierzytelnienia w celu zdezorientowania, wywarcia presji lub wywołania frustracji u użytkownika, tak aby zatwierdził jedno z nich. Jedno przypadkowe zatwierdzenie zwykle wystarczy, aby atakujący otrzymał dostęp.

Dopasowywanie numerów (ang. *number matching*) ogranicza to ryzyko, wymagając od użytkownika wprowadzenia lub wybrania wartości wyświetlanej na ekranie logowania.

© 2026 Rublon

Informacje kontekstowe, takie jak aplikacja, przybliżona lokalizacja, urządzenie i czas wysłania żądania, mogą ułatwić rozpoznanie fałszywych prób.

Mechanizmy te należy łączyć z limitami częstotliwości żądań, tymczasowymi blokadami oraz ograniczeniami dotyczącymi powtarzających się monitów. Administratorzy potrzebują określonej procedury postępowania po kilku nieudanych, odrzuconych lub wygasłych żądaniach. Po odrzuceniu żądania nie powinien natychmiast pojawiać się kolejny identyczny monit.

Siła uwierzytelniania powinna również odpowiadać poziomowi ryzyka związanego z aplikacją. Metoda Powiadomienie mobilne może być odpowiednia dla standardowej usługi, ale konsola administracyjna, system finansowy czy serwer produkcyjny powinny raczej wymagać danych uwierzytelniających zgodnych ze standardem FIDO.

Dzienniki powinny przedstawiać pełną sekwencję żądań, odrzuceń, przekroczeń limitu czasu, zmian metod i zatwierdzeń. Kilka odrzuconych prób, po których następuje jedno skuteczne zatwierdzenie, może wskazywać na trwający atak.

Użytkownicy powinni zostać przeszkoleni w zakresie odrzucania i zgłaszania nieoczekiwanych monitów. Proces zgłaszania powinien określać, z kim należy się skontaktować i jakie działania należy podjąć. Rejestracja i wymiana uwierzytelniaczy wymagają podobnych zabezpieczeń. Weryfikacja tożsamości, zatwierdzanie, rejestrowanie zdarzeń i powiadamianie użytkownika powinny uniemożliwiać atakującym zarejestrowanie nowego telefonu za pomocą socjotechniki.

Pytania do dostawców:

- W jaki sposób ograniczane są powtarzające się ataki wykorzystujące powiadomienia mobilne?
- Czy metoda Powiadomienie mobilne obsługuje dopasowywanie numerów (ang. *number matching*) i informacje kontekstowe?
- Czy metody można ograniczać według użytkownika, grupy lub aplikacji?
- Czy dla systemów wrażliwych można wymagać silniejszych metod?
- Czy podejrzane i odrzucone żądania są widoczne w dziennikach?
- Co dzieje się po powtarzających się niepowodzeniach lub odrzuceniach?
- W jaki sposób weryfikowane są nowe i zastępcze uwierzytelniacze?

3.4. Analiza polityk dostępu i ich egzekwowania

Polityki uwierzytelniania powinny uwzględniać poziom wrażliwości aplikacji, uprawnienia użytkownika, kontekst dostępu oraz ryzyko operacyjne. Jedna reguła obowiązująca w całej organizacji rzadko zapewnia odpowiednią ochronę we wszystkich sytuacjach.

© 2026 Rublon

Polityki dla poszczególnych aplikacji mogą wymagać silniejszego uwierzytelniania w przypadku systemów kadrowo-płacowych, administracyjnych, finansowych lub produkcyjnych. Polityki oparte na użytkownikach i grupach mogą stosować różne mechanizmy zabezpieczeń wobec administratorów, zespołów finansowych, kadry kierowniczej, programistów, wykonawców i użytkowników zewnętrznych.

Ograniczenia metod zapobiegają osłabianiu silniejszych mechanizmów zabezpieczeń przez słabsze opcje. Platforma powinna umożliwiać wymaganie standardu FIDO2 dla wybranych systemów, wyłączanie metod telefonicznych dla użytkowników uprzywilejowanych oraz przeznaczanie kodów tymczasowych wyłącznie do autoryzowanego odzyskiwania dostępu.

Uwierzytelnianie MFA o podwyższonym poziomie (ang. *step-up MFA*) wymaga silniejszej weryfikacji, gdy wzrasta ryzyko, na przykład przed zmianą ustawień bezpieczeństwa, uzyskaniem dostępu do danych podlegających regulacjom lub zatwierdzeniem transakcji finansowej.

Polityki zapamiętanych urządzeń powinny określać kryteria kwalifikacji, okres obowiązywania i warunki unieważnienia zaufania. Użytkownicy i aplikacje wysokiego ryzyka mogą wymagać wyłączenia z takich polityk. Sygnały dotyczące sieci i lokalizacji mogą wpływać na wymagania dotyczące uwierzytelniania, ale nie powinny stanowić jedynej podstawy zaufania.

Konta awaryjne powinny być nieliczne, silnie chronione, testowane i monitorowane. Każde obejście zabezpieczeń musi być tymczasowe i podlegać audytowi.

Należy również jednoznacznie określić zachowanie systemu podczas awarii:

- **Tryb fail-open** zachowuje dostęp, ale umożliwia uwierzytelnianie wyłącznie za pomocą hasła.
- **Tryb fail-closed** utrzymuje wymóg uwierzytelniania MFA, ale może zablokować dostęp uprawnionym użytkownikom.

Odpowiedni model zależy od krytyczności systemu, wpływu na działalność organizacji oraz dostępnych możliwości odzyskiwania dostępu.

Dowiedz się więcej w dokumencie Przewodnik Rublon dotyczący gotowości do zapewnienia ciągłości biznesowej.

Na koniec należy zweryfikować spójność polityk w aplikacjach chmurowych, sieciach VPN, logowaniach do systemu Windows oraz systemach starszego typu. Mechanizm zabezpieczeń widoczny w konsoli może nie być dostępny za pośrednictwem każdej integracji.

© 2026 Rublon

3.5. Weryfikacja możliwości rejestrowania, monitorowania i reagowania na incydenty

Dzienniki uwierzytelniania powinny umożliwiać administratorom odtworzenie przebiegu każdej próby. Podstawowe pola obejmują użytkownika, chroniony zasób, czas, źródłowy adres IP, metodę, wynik zastosowania polityki oraz stan końcowy. Platforma powinna rozróżniać pomyślne uwierzytelnienie, odrzucenie przez użytkownika, przekroczenie limitu czasu, odmowę wynikającą z polityki oraz błąd techniczny.

Równie ważny jest kontekst integracji. Logowanie do aplikacji chmurowej, połączenie z siecią VPN, logowanie do systemu Windows oraz próba dostępu do serwera z systemem Linux za pomocą protokołu SSH stanowią różne ścieżki dostępu.

Zdarzenia dotyczące uwierzytelniaczy powinny obejmować rejestrację telefonu, rejestrację klucza bezpieczeństwa, wymianę, unieważnienie i dostęp tymczasowy. Rejestry powinny wskazywać, kto zainicjował działanie i kiedy miało ono miejsce. W miarę możliwości użytkownicy powinni być powiadamiani o istotnych zmianach.

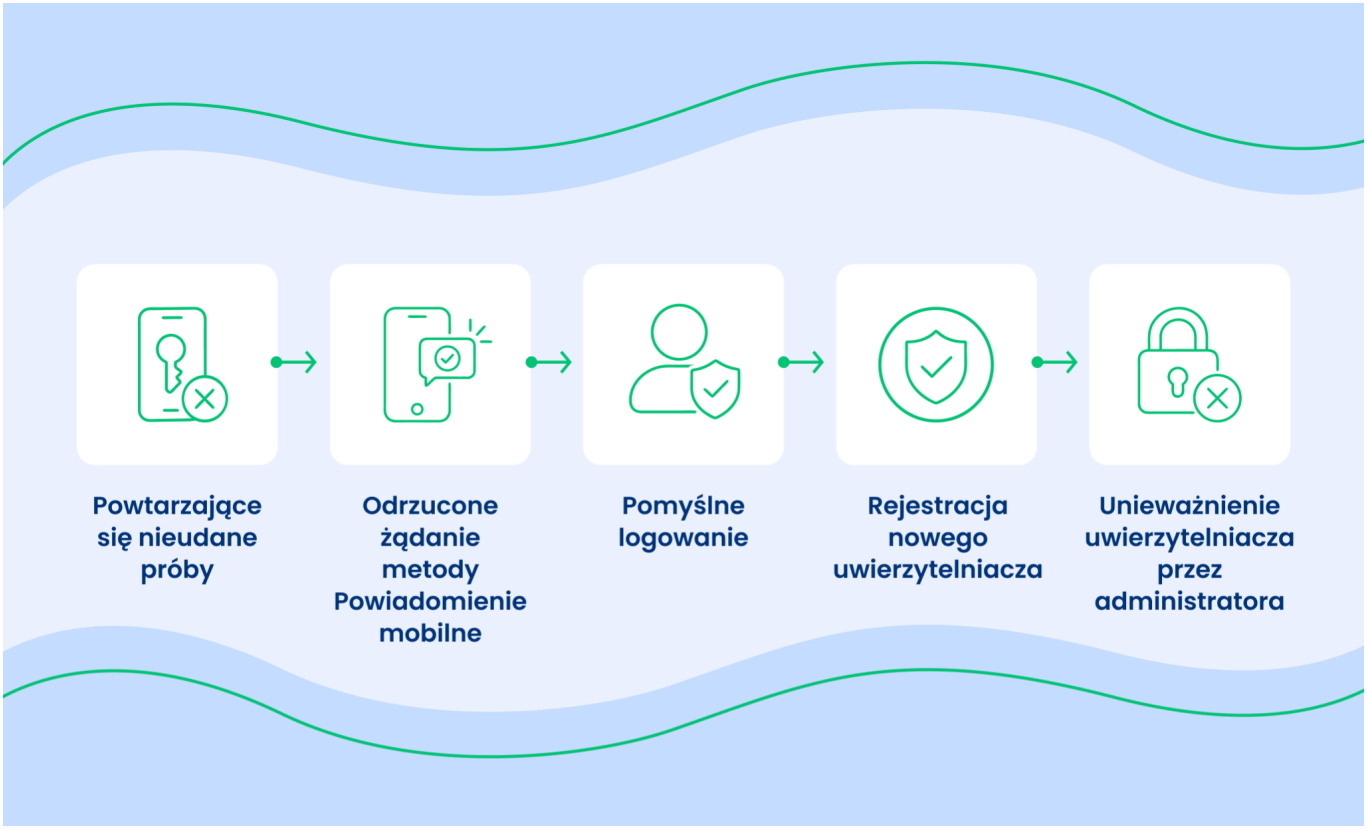
Administracyjne dzienniki audytu powinny rejestrować zmiany polityk, aplikacji, ról, stanu użytkowników, synchronizacji katalogów oraz ustawień bezpieczeństwa. Pomaga to ustalić, czy mechanizm zabezpieczeń zawiódł, został nieprawidłowo skonfigurowany, czy celowo zmieniony.

Dzienniki powinny umożliwiać wyszukiwanie, być przechowywane przez odpowiedni okres oraz nadawać się do eksportu do platformy SIEM. W przypadku podejrzenia przejęcia konta administratorzy powinni mieć możliwość unieważnienia uwierzytelniaczy, usunięcia zaufania do zapamiętanych urządzeń, wyłączenia metod i wymuszenia bezpiecznej ponownej rejestracji. Działania podejmowane w ramach reagowania również muszą podlegać audytowi.

Pytania, które należy zadać:

- Co jest rejestrowane dla każdej próby?
- Czy można rozróżnić odrzucenie, przekroczenie limitu czasu, odmowę wynikającą z polityki i błąd techniczny?
- Czy zdarzenia rejestracji, wymiany i unieważnienia są zapisywane w dziennikach?
- Czy wszystkie zmiany administracyjne podlegają audytowi?
- Jak długo przechowywane są rejestry?
- Czy dzienniki można automatycznie eksportować do platformy SIEM?
- Czy uwierzytelniacze i zapamiętane urządzenia można szybko unieważnić?
- Czy dostępne dowody są wystarczające na potrzeby postępowań wyjaśniających i audytów?

© 2026 Rublon



Pełny obraz chronologicznej historii aktywności MFA wymaga rejestrowania zarówno prób uwierzytelniania, jak i zdarzeń związanych z cyklem życia uwierzytelniaczy.

4. Ocena zakresu ochrony infrastruktury i integracji

4.1. Ochrona środowisk chmurowych, lokalnych i hybrydowych

Większość organizacji korzysta z kilku modeli zarządzania tożsamością i uwierzytelniania. Usługi chmurowe mogą korzystać z federacji tożsamości, podczas gdy aplikacje wewnętrzne nadal wykorzystują usługę Active Directory, LDAP, RADIUS, konta lokalne lub starsze mechanizmy logowania. Użytkownicy zdalni łączą się za pośrednictwem sieci VPN i bram, a administratorzy mogą logować się bezpośrednio do systemów Windows lub Linux.

Rozwiązanie MFA przeznaczone wyłącznie do środowisk chmurowych może zatem pozostawiać poza granicami ochrony lokalne stacje robocze, serwery, urządzenia sieciowe i aplikacje starszego typu.

Odpowiednia platforma powinna zapewniać scentralizowane zarządzanie politykami i widoczność zdarzeń, a jednocześnie obsługiwać różne mechanizmy egzekwowania uwierzytelniania. Powinna współdziałać z istniejącymi usługami katalogowymi i dostawcami

© 2026 Rublon

tożsamości, wykorzystywać uznane protokoły tam, gdzie jest to właściwe, oraz oferować dedykowane konektory, gdy wymagana jest głębsza integracja.

Modernizacja powinna przebiegać stopniowo. Nowe aplikacje mogą wdrażać standard SAML lub protokół OpenID Connect, podczas gdy starsze systemy pozostają chronione za pomocą protokołu LDAP, protokołu RADIUS, lokalnych konektorów lub bram. Obsługa obu modeli pozwala uniknąć powielania zadań administracyjnych i rozproszenia narzędzi bezpieczeństwa.

Ochrona środowiska hybrydowego ułatwia również prowadzenie postępowań wyjaśniających. Wspólny widok uwierzytelniania w usługach chmurowych, sieciach VPN, serwerach i urządzeniach końcowych ułatwia śledzenie aktywności w różnych ścieżkach dostępu oraz identyfikowanie niespójnego egzekwowania zabezpieczeń.

Należy oceniać konkretne aplikacje, systemy operacyjne, protokoły i scenariusze logowania. Ogólne deklaracje dotyczące obsługi środowisk chmurowych lub lokalnych nie są wystarczające.



Scentralizowana platforma MFA pozwala objąć wspólną ochroną zasoby chmurowe, lokalne i zdalne w środowisku hybrydowym.

© 2026 Rublon

4.2. Ocena zakresu integracji

Zakres integracji należy oceniać na podstawie rzeczywistych ścieżek dostępu w organizacji, a nie liczby logo produktów na stronie dostawcy.

Systemy dostępu zdalnego, takie jak sieci VPN, zapory sieciowe, kontrolery sieci bezprzewodowych i urządzenia sieciowe, często korzystają z protokołu RADIUS lub protokołu LDAP. Zgodność należy zweryfikować dla konkretnej wersji produktu, trybu uwierzytelniania i architektury sieciowej. Systemy korzystające z tego samego protokołu mogą w różny sposób obsługiwać żądania uwierzytelnienia, limity czasu i uwierzytelnianie dodatkowe.

Zakres ochrony systemu Windows należy oceniać oddzielnie dla następujących scenariuszy:

- Local Windows Logon
- Remote Desktop Protocol
- Remote Desktop Gateway
- Remote Desktop Web Access i Web Client
- Inne usługi firmy Microsoft i administracyjne ścieżki dostępu

W przypadku systemu Linux należy zweryfikować obsługę modułów PAM i protokołu SSH, w tym sesji interaktywnych, dostępu uprzywilejowanego, kluczy SSH, kont automatyzacji oraz scenariuszy odzyskiwania dostępu.

Aplikacje chmurowe i webowe mogą korzystać z natywnych konektorów, standardu SAML, protokołu OAuth 2.0, protokołu OpenID Connect, bram dostępu, odwrotnych serwerów proxy lub innych komponentów. Wybrane podejście powinno zachowywać prawidłowe działanie aplikacji i umożliwiać dalsze wsparcie po aktualizacjach.

Aplikacje niestandardowe mogą wymagać interfejsów API lub zestawów SDK. Należy przeanalizować obsługiwane języki programowania, przykłady, obsługę błędów, politykę wydań, zgodność wsteczną oraz odpowiedzialność za utrzymanie.

Nie należy pomijać konsol administracyjnych, platform wirtualizacyjnych, systemów kopii zapasowych, hiperwizorów, baz danych i narzędzi bezpieczeństwa. Związane z nimi uprawnienia często sprawiają, że stanowią one większe ryzyko niż standardowe aplikacje używane przez pracowników.

Zgodność ze źródłami tożsamości może obejmować usługę Active Directory, usługę Microsoft Entra ID, katalogi korzystające z protokołu LDAP, usługi oparte na protokole RADIUS, dostawców tożsamości korzystających ze standardu SAML oraz tożsamości lokalne.

© 2026 Rublon



Kryteria oceny

Dla każdej integracji należy określić:

- Czy wykorzystuje natywny konektor, protokół, federację tożsamości, bramę czy kod niestandardowy
- Obsługiwane wersje aplikacji i systemów operacyjnych
- Dostępność dokumentacji dotyczącej konfiguracji i rozwiązywania problemów
- Obsługiwane metody uwierzytelniania
- Wymagania dotyczące komponentów lokalnych i certyfikatów
- Polityki aktualizacji i zgodności wstecznej
- Opcje wysokiej dostępności
- Odpowiedzialność za utrzymanie
- Doświadczenie użytkownika
- Znane ograniczenia i nieobsługiwane scenariusze

Obsługa metod może różnić się w zależności od integracji. Standard FIDO2 może być dostępny dla aplikacji webowej, ale dla określonego rozwiązania VPN może być obsługiwana wyłącznie metoda Powiadomienie mobilne lub kody TOTP. Obsługiwane metody należy rejestrować oddzielnie dla każdej ścieżki dostępu.

4.3. Sprawdzenie zgodności protokołów i źródeł tożsamości

Platforma MFA powinna współpracować z istniejącą architekturą tożsamości bez konieczności natychmiastowego migrowania usługi katalogowej.

© 2026 Rublon

Obsługa usługi Active Directory powinna obejmować wykrywanie użytkowników, mapowanie grup, zmiany stanu kont oraz środowiska domenowe. Usługa Microsoft Entra ID może działać jako główne chmurowe źródło tożsamości lub współistnieć z usługą Active Directory.

Protokoły LDAP i LDAPS zapewniają zgodność z firmowymi usługami katalogowymi. Należy zweryfikować wymagania dotyczące schematu, bazy wyszukiwania, mapowania atrybutów, uprawnień konta usługi, weryfikacji certyfikatów oraz zachowania w przypadku awarii usługi katalogowej. Należy preferować protokół LDAPS, tam, gdzie jest obsługiwany.

Protokół RADIUS jest powszechnie używany przez sieci VPN, zapory sieciowe, systemy sieci bezprzewodowych i urządzenia sieciowe. Z uwagi na to, że jest to protokół uwierzytelniania, a nie usługa katalogowa, należy ustalić, w jaki sposób weryfikowane są podstawowe dane uwierzytelniające oraz jak obsługiwane są żądania uwierzytelniania MFA, limity czasu i przełączanie awaryjne.

Standard SAML obsługuje uwierzytelnianie federacyjne w wielu aplikacjach chmurowych i internetowych. Protokół OAuth 2.0 służy do autoryzacji, natomiast protokół OpenID Connect rozszerza ten mechanizm o uwierzytelnianie. Deklaracje dostawcy powinny wskazywać obsługiwane role i przepływy.

Synchronizacja katalogów powinna importować użytkowników i grupy, szybko stosować zmiany oraz zgłaszać błędy. Wiele usług katalogowych i domen wymaga niezawodnego dopasowywania tożsamości. W przeciwnym razie zduplikowane nazwy użytkowników, zmieniające się adresy e-mail oraz fuzje organizacji mogą powodować konflikty lub nieprawidłowe łączenie kont.

Równie ważne są procesy aprowizacji i wycofywania dostępu. Użytkownicy, których konta zostały wyłączone lub usunięte, powinni szybko tracić dostęp.

Pytania, które należy zadać:

- Czy można zachować istniejące źródła tożsamości?
- Czy wymagana jest firmowa usługa katalogowa dostawcy?
- Czy możliwe jest współistnienie wielu usług katalogowych, domen i dostawców tożsamości?
- W jaki sposób rozwiązywane są konflikty tożsamości?
- Jak szybko synchronizowane są zmiany?
- Co się dzieje, gdy konto zostanie wyłączone, usunięte lub przeniesione?
- Czy zgłaszane są błędy synchronizacji?
- Który system pozostaje nadrzędnym źródłem danych?

© 2026 Rublon



Scentralizowana platforma MFA może współpracować z istniejącymi źródłami tożsamości i centralizować najważniejsze funkcje zarządzania.

4.4. Ocena obsługi aplikacji niestandardowych i aplikacji typu legacy

Starsze i opracowane wewnętrznie systemy typu legacy często są najtrudniejsze do zabezpieczenia i najłatwiejsze do pominięcia.

Najpierw należy ocenić protokoły i standardy ogólnego przeznaczenia, takie jak protokół RADIUS, protokół LDAP, standard SAML, protokół OAuth 2.0 i protokół OpenID Connect. Standardy mogą ograniczyć nakład pracy programistycznej, ale zgodność należy przetestować z rzeczywistym przepływem uwierzytelniania.

Interfejsy API i zestawy SDK mogą służyć do integrowania uwierzytelniania MFA z niestandardowymi procesami logowania, działaniami uprzywilejowanymi lub zatwierdzaniem transakcji. Należy ocenić obsługiwane języki programowania, przykładowy kod, sposób wersjonowania, obsługę błędów oraz obowiązki w zakresie bezpieczeństwa przypisane programistom.

Do zabezpieczenia aplikacji internetowych, których nie można modyfikować mogą zostać wykorzystane odwrotne serwery proxy (ang. *reverse proxy*) i bramy dostępu (ang. *access*

© 2026 Rublon

gateway). Należy przeanalizować obsługę sesji, certyfikaty, przekierowania, zachowanie źródłowego adresu IP klienta, dostępność oraz zgodność z aktualizacjami.

Jeżeli systemu nie można zmodyfikować, można wdrożyć egzekwowanie MFA na innej warstwie, takiej jak sieć VPN, logowanie do systemu operacyjnego, brama dostępu zdalnego, granica sieci lub interfejs administracyjny.

Przed wyborem rozwiązania należy oszacować nakład pracy związany z tworzeniem i utrzymaniem integracji niestandardowej. Trzeba również przypisać odpowiedzialność za jej opracowanie, przetestowanie i aktualizowanie.

Opcje oparte na standardach, udokumentowane interfejsy API i możliwe do oddzielenia warstwy integracji mogą ograniczyć uzależnienie od dostawcy, natomiast integracje natywne mogą zapewnić bardziej szczegółową kontrolę tam, gdzie jest to uzasadnione.

Nie należy oceniać wyłącznie aplikacji, które łatwo zabezpieczyć. Należy również ocenić systemy, które po wdrożeniu nadal korzystałyby wyłącznie z haseł.

5. Ocena doświadczenia użytkowników i administratorów

5.1. Doświadczenie związane z uwierzytelnianiem

Proces uwierzytelniania należy oceniać na podstawie liczby działań wykonywanych przez użytkownika, czasu potrzebnego na jego ukończenie, zrozumiałości oraz spójności między aplikacjami.

W przypadku rutynowego logowania uzasadnione może być zastosowanie metody powodującej niewielkie utrudnienia, natomiast dostęp uprzywilejowany może wymagać silniejszej weryfikacji. Powtarzające się monity, które w niewielkim stopniu zwiększają bezpieczeństwo, skłaniają użytkowników do pośpiesznego działania lub szukania sposobów obejścia zabezpieczeń.

Przebieg uwierzytelniania będzie różnić się w zależności od przeglądarki, klienta sieci VPN, logowania do systemu Windows, sesji z użyciem protokołu SSH oraz urządzenia mobilnego, ale użytkownicy powinni zawsze rozumieć, jakie działanie jest od nich wymagane. Komunikaty o błędach powinny rozróżniać odrzucenie żądania, wygaśnięcie, ograniczenie wynikające z polityki, nieprawidłowe kody dostępu, awarie usługi oraz błędy techniczne.

Należy przetestować procesy na urządzeniach mobilnych i komputerach. Niektórzy użytkownicy nie będą mieć firmowych smartfonów, będą pracować w strefach objętych ograniczeniami lub

© 2026 Rublon

nie zgodzą się na używanie urządzeń prywatnych. Powinny być dostępne odpowiednie alternatywy, które nie obniżają poziomu ochrony wszystkich użytkowników.

Należy poznać wymagania dotyczące łączności. Kody TOTP i niektóre lokalne uwierzytelniacze działają bez dostępu do danych komórkowych, podczas gdy inne metody wymagają połączenia z usługą chmurową.

Współdzielone stacje robocze muszą zapewniać oddzielenie tożsamości, sesji oraz stanu zapamiętanego urządzenia. Wymagania dotyczące dostępności powinny obejmować rejestrację, uwierzytelnianie, obsługę błędów i odzyskiwanie dostępu.

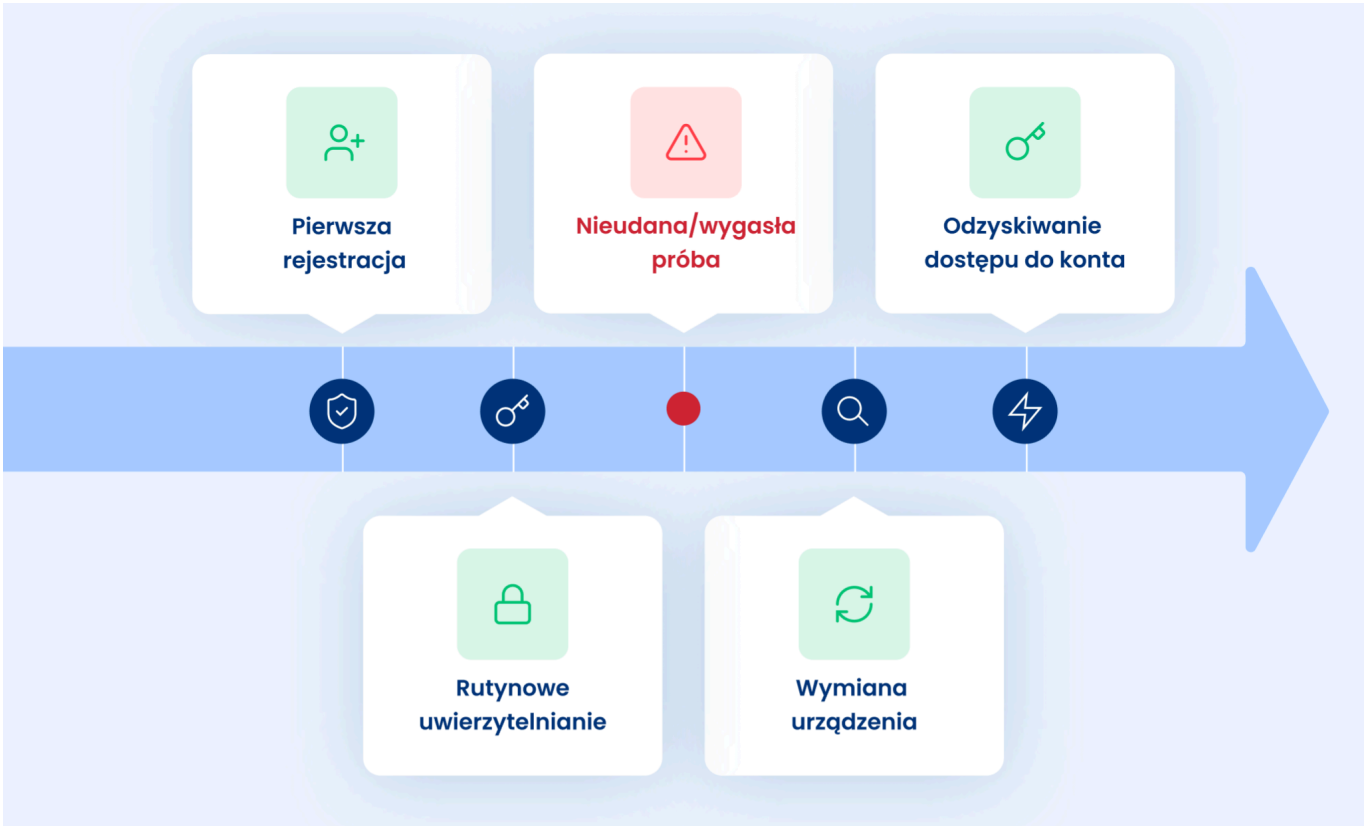
Korzystanie z wielu uwierzytelniaczy pomaga zwiększyć odporność. Użytkownik może na co dzień korzystać z klucza dostępu, zachować klucz bezpieczeństwa jako metodę zapasową oraz używać innej zatwierdzonej metody w przypadku określonych systemów.

Testy podczas weryfikacji koncepcji:

- Pierwsze uwierzytelnienie po rejestracji
- Rutynowe uwierzytelnianie w kilku aplikacjach
- Odrzucenie żądania przez użytkownika
- Wygaśnięcie żądania
- Utrata łączności
- Migracja na nowy telefon
- Utrata klucza bezpieczeństwa
- Zablokowane lub wyłączone konto
- Pełny proces odzyskiwania dostępu

Należy rejestrować czas ukończenia procesu, problemy użytkowników ze zrozumieniem wymaganych działań, konieczność interwencji działu pomocy technicznej oraz różnice między integracjami.

© 2026 Rublon



Cykl życia uwierzytelniacza obejmuje rejestrację, rutynowe użycie, obsługę nieudanych prób, wymianę urządzenia i odzyskiwanie dostępu.

5.2. Rejestracja i cykl życia uwierzytelniacza

Rejestracja łączy tożsamość z uwierzytelniaczem. Niewłaściwie zabezpieczony proces rejestracji może spowodować przypisanie silnych danych uwierzytelniających do niewłaściwej osoby.

Rejestracja przeprowadzana przez administratora zapewnia większą kontrolę w przypadku użytkowników uprzywilejowanych, kluczy bezpieczeństwa, tokenów sprzętowych i środowisk podlegających regulacjom, ale może być trudna do zastosowania na dużą skalę. Samodzielna rejestracja ogranicza nakład pracy administracyjnej, pod warunkiem że zaproszenia są chronione, ograniczone czasowo i powiązane z wiarygodną weryfikacją tożsamości.

Rejestracja zbiorcza powinna przyspieszać wdrożenie bez automatycznego uznawania niezweryfikowanych urządzeń za zaufane. Administratorzy potrzebują informacji o kontach, dla których rejestracja została ukończona, pozostaje w toku lub nie jest wymagana ze względu na przyznany wyjątek.

© 2026 Rublon

Użytkownicy mogą potrzebować wielu uwierzytelniaczy w celu zwiększenia odporności. Polityki powinny określać dozwolone typy, limity rejestracji oraz wymagania dotyczące metod zapasowych dla użytkowników wysokiego ryzyka.

Wymiana uwierzytelniacza i odzyskiwanie dostępu wymagają silnej weryfikacji. W przypadku utraty telefonu lub klucza należy unieważnić stary uwierzytelniacz, przeanalizować ostatnią aktywność i powiadomić użytkownika. Metody dostępu tymczasowego powinny automatycznie wygasać i podlegać pełnemu audytowi.

Proces odejścia użytkownika z organizacji powinien prowadzić do szybkiego unieważnienia uwierzytelniaczy, zapamiętanych urządzeń, wyjątków oraz metod odzyskiwania dostępu. Synchronizacja usługi katalogowej może wspierać ten proces, ale należy przetestować opóźnienia i sposób obsługi błędów.

Mechanizmy ochrony przed nieautoryzowaną rejestracją powinny obejmować ograniczone uprawnienia administracyjne, zatwierdzanie, powiadomienia oraz kompletne rejestry audytowe.

5.3. Doświadczenie administratorów i delegowanie uprawnień

Scentralizowana konsola powinna umożliwiać zarządzanie użytkownikami, aplikacjami, politykami, uwierzytelniaczami i zdarzeniami związanymi z bezpieczeństwem bez konieczności odtwarzania informacji z wielu narzędzi.

Rekordy użytkowników powinny zawierać stan, aplikacje, grupy, uwierzytelniacze, przypisane polityki oraz ostatnią aktywność. Właściciele aplikacji potrzebują podobnej widoczności chronionych zasobów i przypisanych polityk.

Dostęp administracyjny powinien być zgodny z zasadą najmniejszych uprawnień (ang. *principle of least privilege*). Właściciele platformy mogą wymagać pełnej kontroli, natomiast pracownicy działu pomocy technicznej powinni mieć możliwość unieważnienia utraconego uwierzytelniacza lub przyznania dostępu tymczasowego bez możliwości zmieniania polityk obowiązujących w całej organizacji.

Podział obowiązków może rozgraniczać zarządzanie bezpieczeństwem, infrastrukturą, pomocą techniczną, rozliczeniami i aplikacjami. Jednostki administracyjne mogą dodatkowo ograniczać dostęp według działu, regionu, spółki zależnej, klienta lub dzierżawcy.

Operacje zbiorcze, wyszukiwanie i filtrowanie powinny wspierać duże wdrożenia. Administratorzy muszą mieć możliwość znajdowania kont według stanu, źródła tożsamości, grupy, typu uwierzytelniacza i stanu rejestracji.

© 2026 Rublon

Informacje dostępne podczas rozwiązywania problemów powinny wskazywać, która polityka została zastosowana, jakiej metody próbowano użyć oraz dlaczego uwierzytelnianie zakończyło się niepowodzeniem. Błędy usługi katalogowej, awarie konektorów, przekroczenia limitu czasu, odrzucenia żądań i odmowy wynikające z polityk wymagają różnych działań.

Wszystkie działania administracyjne powinny być przypisane do konkretnych osób i oznaczone znacznikiem czasu. Same konta administracyjne powinny korzystać z silnego uwierzytelniania MFA. Środowiska wielodostępne wymagają również wyraźnie określonych granic raportowania oraz zabezpieczeń przed wprowadzaniem zmian w niewłaściwej organizacji.

Pytania, które należy zadać:

- Ile konsol jest wymaganych?
- Czy uprawnienia można ograniczać według roli, zadania i zakresu?
- Czy pracownicy działu pomocy technicznej mogą odzyskać dostęp bez zmieniania polityk?
- Czy dostępne są operacje zbiorcze?
- Czy administratorzy mogą ustalić przyczynę nieudanego uwierzytelnienia?
- Czy wszystkie zmiany administracyjne podlegają audytowi?
- Czy od administratorów wymagane jest uwierzytelnianie MFA?
- Czy dzierżawcy i dane klientów są od siebie odizolowane?

6. Ocena wdrożenia i eksploatacji

6.1. Architektura wdrożenia

Architektura wdrożenia określa, gdzie przetwarzane są dane uwierzytelniające, gdzie podejmowane są decyzje dotyczące uwierzytelniania oraz w jaki sposób chronione systemy komunikują się z platformą MFA.

Platforma zarządzana w chmurze może centralizować konfigurację, polityki, administrację i dzienniki. Lokalne konektory mogą nadal egzekwować uwierzytelnianie MFA w sieciach VPN, usługach katalogowych, systemach Windows, serwerach z systemem Linux oraz aplikacjach wewnętrznych.

W modelu hybrydowym centralne polityki są połączone z komponentami wdrożonymi w pobliżu chronionych zasobów. Dokumentacja architektury powinna określać funkcję każdego komponentu, przetwarzane dane oraz zachowanie w przypadku przerwania łączności.

Należy przeanalizować:

- Wymagania sieciowe dotyczące połączeń wychodzących i przychodzących

© 2026 Rublon

- Reguły zapory sieciowej i udostępnione porty
- Zgodność z serwerami proxy
- Certyfikaty protokołu TLS i sposób przechowywania kluczy prywatnych
- Odnawianie certyfikatów i monitorowanie terminów ich wygaśnięcia
- Uprawnienia kont usługowych i rotację danych uwierzytelniających
- Przepływy danych, lokalizacje przetwarzania, okresy przechowywania i lokalizację danych
- Dostawców usług hostingowych, podmioty przetwarzające i kopie zapasowe
- Wzmacnianie zabezpieczeń komponentów i instalowanie poprawek

Połączenia wychodzące są zazwyczaj łatwiejsze do zabezpieczenia, natomiast dostęp przychodzący powinien być uzasadniony i ograniczony do minimum.

Konta usługowe powinny otrzymywać wyłącznie uprawnienia wymagane do realizacji ich zadań. Dostęp do usługi katalogowej, integracje, rejestrowanie zdarzeń i administracja mogą wymagać oddzielnych tożsamości.

W przypadku komponentów lokalnych należy wyłączyć zbędne usługi, ograniczyć dostęp administracyjny, monitorować dzienniki oraz określić procedury aktualizacji.

Należy również rozdzielić warstwę zarządzania od warstwy uwierzytelniania. Utrata dostępu do konsoli administracyjnej nie powinna automatycznie zatrzymywać uwierzytelniania, natomiast przejęcie jednego konektora nie powinno zapewniać kontroli nad całą platformą.

Przykład: Przeczytaj o architekturze rozwiązania Rublon MFA.

6.2. Czas wdrożenia i czas do osiągnięcia ochrony

Czas do osiągnięcia ochrony to okres między wyborem platformy a uzyskaniem zweryfikowanej ochrony ważnych ścieżek dostępu.

Należy rozpocząć od rozpoznania użytkowników, źródeł tożsamości, aplikacji, protokołów, zależności i scenariuszy wyjątkowych. Niepełne rozpoznanie prowadzi do opóźnień i wykrywania nieobsługiwanych przypadków użycia podczas wdrożenia.

Weryfikacja koncepcji powinna obejmować co najmniej jeden system krytyczny, jedno reprezentatywne źródło tożsamości, wymagane metody, polityki, dzienniki, odzyskiwanie dostępu oraz zachowanie podczas awarii. Następnie program pilotażowy powinien objąć administratorów, pracowników biurowych, pracowników zdalnych oraz użytkowników o nietypowych wymaganiach dotyczących urządzeń lub łączności.

© 2026 Rublon

Wdrożenie produkcyjne jest bezpieczniejsze, gdy przebiega w kontrolowanych etapach. Każdy etap wymaga kryteriów rozpoczęcia, mierników powodzenia, określenia odpowiedzialności za pomoc techniczną oraz przetestowanego planu wycofania zmian.

Komunikację należy rozpocząć przed włączeniem egzekwowania zabezpieczeń. Użytkownicy potrzebują informacji o terminach rejestracji, dostępnych metodach i danych kontaktowych działu pomocy technicznej. Administratorzy i zespoły pomocy technicznej wymagają szkolenia z rozwiązywania problemów, odzyskiwania dostępu i eskalacji.

Poziom wdrożenia należy mierzyć za pomocą wskaźników rejestracji, wykorzystania wymaganych metod, liczby chronionych aplikacji, nieudanych rejestracji, wyjątków oraz kont korzystających wyłącznie z haseł.

Sugerowana kolejność wdrożenia:

1. Administratorzy i pracownicy działu IT
2. Dostęp zdalny i sieci VPN
3. Serwery krytyczne i systemy uprzywilejowane
4. Aplikacje chmurowe i internetowe
5. Pozostałe aplikacje używane przez pracowników
6. Systemy starszego typu i wyjątkowe przypadki użycia

Priorytety należy ustalać na podstawie ryzyka, a nie łatwości wdrożenia.

© 2026 Rublon



Skuteczne wdrożenie MFA przebiega etapami: od rozpoznania i weryfikacji koncepcji po wdrożenie produkcyjne i ciągłą optymalizację.

6.3. Dostępność, odporność i odzyskiwanie

Uwierzytelnianie MFA stanowi część ścieżki dostępu do systemów krytycznych. Zakłócenie może zablokować uprawnionych użytkowników lub obniżyć poziom bezpieczeństwa przez ominięcie uwierzytelniania.

Należy przeanalizować formalną umowę SLA, metodę obliczania poziomu dostępności, wyłączenia, nadmiarowość, rozmieszczenie geograficzne, przełączanie awaryjne, kopie zapasowe oraz procedury odzyskiwania.

Lokalne serwery proxy, bramy, konektory i usługi katalogowe mogą stanowić pojedyncze punkty awarii. Należy potwierdzić obsługę nadmiarowych instancji, równoważenia obciążenia i synchronizacji konfiguracji.

Należy określić zachowanie uwierzytelniania podczas:

- Awarii usługi chmurowej
- Awarii konektora
- Awarii usługi katalogowej

© 2026 Rublon

- Zakłócenia działania sieci
- Ograniczonej łączności
- Planowanych prac konserwacyjnych

W przypadku uwierzytelniania w trybie offline należy określić obsługiwanych użytkowników, metody, systemy, okresy ważności oraz wymagania audytowe.

Monitorowanie powinno wskazywać, czy komponenty są osiągalne, prawidłowo skonfigurowane i przetwarzają żądania. Komunikaty o błędach powinny rozróżniać problemy z usługą katalogową, konektorem, siecią i usługą MFA.

Decyzje dotyczące trybu fail-open i trybu fail-closed muszą być zatwierdzane oddzielnie dla każdego systemu. Krytyczne systemy opieki zdrowotnej, bezpieczeństwa, produkcji i służb ratunkowych mogą wymagać innych modeli ciągłości działania niż standardowe aplikacje.

Polityki, konfiguracje konektorów, certyfikaty, konta usługowe i sekrety powinny być objęte kopiami zapasowymi oraz możliwe do odzyskania. Należy udokumentować odpowiedzialność za odzyskiwanie, cele, zależności i częstotliwość testów.

Dostawca powinien utrzymywać kanał informujący o stanie usług oraz przekazywać w odpowiednim czasie informacje o incydentach, rozwiązaniach tymczasowych i działaniach podjętych po incydencie, gdy jest to uzasadnione.

6.4. Wymagania dotyczące utrzymania i aktualizacji

Należy określić, które komponenty są utrzymywane przez dostawcę, a które pozostają w zakresie odpowiedzialności klienta.

Usługi chmurowe mogą być aktualizowane automatycznie, podczas gdy konektory, agenty, bramy i wtyczki wymagają lokalnego utrzymania. Automatyczne aktualizacje ograniczają rutynowe prace, ale mogą powodować ryzyko problemów ze zgodnością. Aktualizacje ręczne zapewniają kontrolę tylko wtedy, gdy nowe wersje są monitorowane i instalowane bez zbędnej zwłoki.

Należy potwierdzić:

- Obsługiwane systemy operacyjne i wersje aplikacji
- Okresy wsparcia dla starszych platform
- Terminy zapewniania zgodności z nowymi wersjami
- Procesy instalowania poprawek zabezpieczeń i aktualizacji awaryjnych
- Zgodność wsteczną
- Powiadomienia o nowych wersjach i wycofaniu obsługi

© 2026 Rublon

- Wymagania dotyczące okien konserwacyjnych

Testy aktualizacji powinny obejmować podstawowe uwierzytelnianie, uwierzytelnianie MFA, polityki, dzienniki, przełączanie awaryjne i odzyskiwanie. W środowiskach wysokiej dostępności należy w miarę możliwości umożliwić sekwencyjne aktualizowanie komponentów.

Model odpowiedzialności powinien obejmować utrzymanie usług chmurowych, lokalne monitorowanie, aktualizowanie konektorów, odnawianie certyfikatów, weryfikowanie chronionych aplikacji oraz zależności od podmiotów zewnętrznych.

7. Ocena aspektów handlowych i dostawcy

7.1. Obliczanie całkowitego kosztu posiadania

Cena subskrypcji jest tylko jednym z elementów kosztu rozwiązania MFA. Należy porównać wszystkie wydatki związane z wdrożeniem, eksploatacją, obsługą i rozszerzaniem platformy.

Należy przeanalizować sposób przypisywania licencji, obowiązywanie minimalnych zobowiązań oraz sposób obsługi wykonawców, użytkowników sezonowych, kont usługowych, nieaktywnych użytkowników i ponownie przypisywanych licencji.

Opłaty za poszczególne metody należy oddzielić od podstawowej opłaty za subskrypcję. Uwierzytelnianie za pomocą wiadomości SMS i połączeń telefonicznych może generować koszty zależne od częstotliwości użycia, kraju docelowego oraz sposobu działania metod zapasowych.

Sprzętowe klucze bezpieczeństwa i tokeny OTP generują koszty zakupu, wysyłki, zarządzania zapasami, wymiany oraz utrzymywania urządzeń zapasowych. Czas pracy administracyjnej często generuje większe koszty niż widoczna cena urządzenia.

Dodatkowe kategorie kosztów obejmują:

- Licencje na aplikacje i konektory
- Płatne protokoły lub moduły
- Licencje na funkcje wysokiej dostępności
- Środowiska testowe i programistyczne
- Usługi profesjonalne
- Prace związane z integracjami niestandardowymi
- Pakiety wsparcia technicznego
- Maszyny wirtualne i licencje na systemy operacyjne
- Bazy danych, moduły równoważenia obciążenia, certyfikaty, systemy monitorowania i kopie zapasowe

© 2026 Rublon

- Wewnętrzne prace związane z wdrożeniem i administracją
- Szkolenia i komunikację
- Utrzymanie konektorów
- Obciążenie działu pomocy technicznej
- Uwierzytelniacze zastępcze

Należy oszacować zapotrzebowanie na pomoc techniczną związane ze zgubionymi urządzeniami, zmianą telefonów, zapomnianymi kodami PIN, nieudaną rejestracją, zablokowanymi kontami i dostępem tymczasowym.

Model powinien uwzględniać rozwój wynikający z dodawania nowych użytkowników, biur, przejmowanych organizacji, aplikacji, źródeł tożsamości i metod uwierzytelniania.

Trzyletni model TCO:

Należy stosować jednolite założenia wobec wszystkich dostawców. Zamiast polegać wyłącznie na najniższych stawkach ofertowych, warto dokumentować wszelkie niepewności oraz analizować scenariusze wzmożonego użycia i wzrostu.

Kategoria kosztów	Rok 1	Rok 2	Rok 3	Założenia
Wdrożenie początkowe				Architektura, integracja, testowanie, migracja
Roczna subskrypcja				Użytkownicy, zobowiązania, przewidywany rozwój
Realizacja uwierzytelnia nia				Wykorzystanie wiadomości SMS i połączeń telefonicznych według kraju i wolumenu
Uwierzytelnia cze sprzętowe				Zakupy, urządzenia zapasowe, wysyłka, wymiana
Wewnętrzny nakład pracy				Wdrożenie, administracja, szkolenia, pomoc techniczna

© 2026 Rublon

Wsparcie techniczne i utrzymanie				Wsparcie dostawcy, infrastruktura, aktualizacje, certyfikaty
Rozszerzenie				Użytkownicy, aplikacje, komponenty, usługi

7.2. Zapewnienie bezpieczeństwa, prywatność i zgodność

Z uwagi na to, że dostawca rozwiązania MFA stanowi część ścieżki uwierzytelniania i przetwarza dane istotne z punktu widzenia bezpieczeństwa, wymagane są dowody potwierdzające stosowane przez niego mechanizmy zabezpieczeń.

Niezależne certyfikaty, takie jak certyfikat zgodności z normą ISO/IEC 27001, oraz raporty, takie jak raport SOC 2, mogą stanowić potwierdzenie bezpieczeństwa, ale istotny jest ich zakres. Należy zweryfikować objęty nimi podmiot prawny, usługi, okres audytu, audytora oraz wyłączenia.

Należy przeanalizować stosowane przez dostawcę:

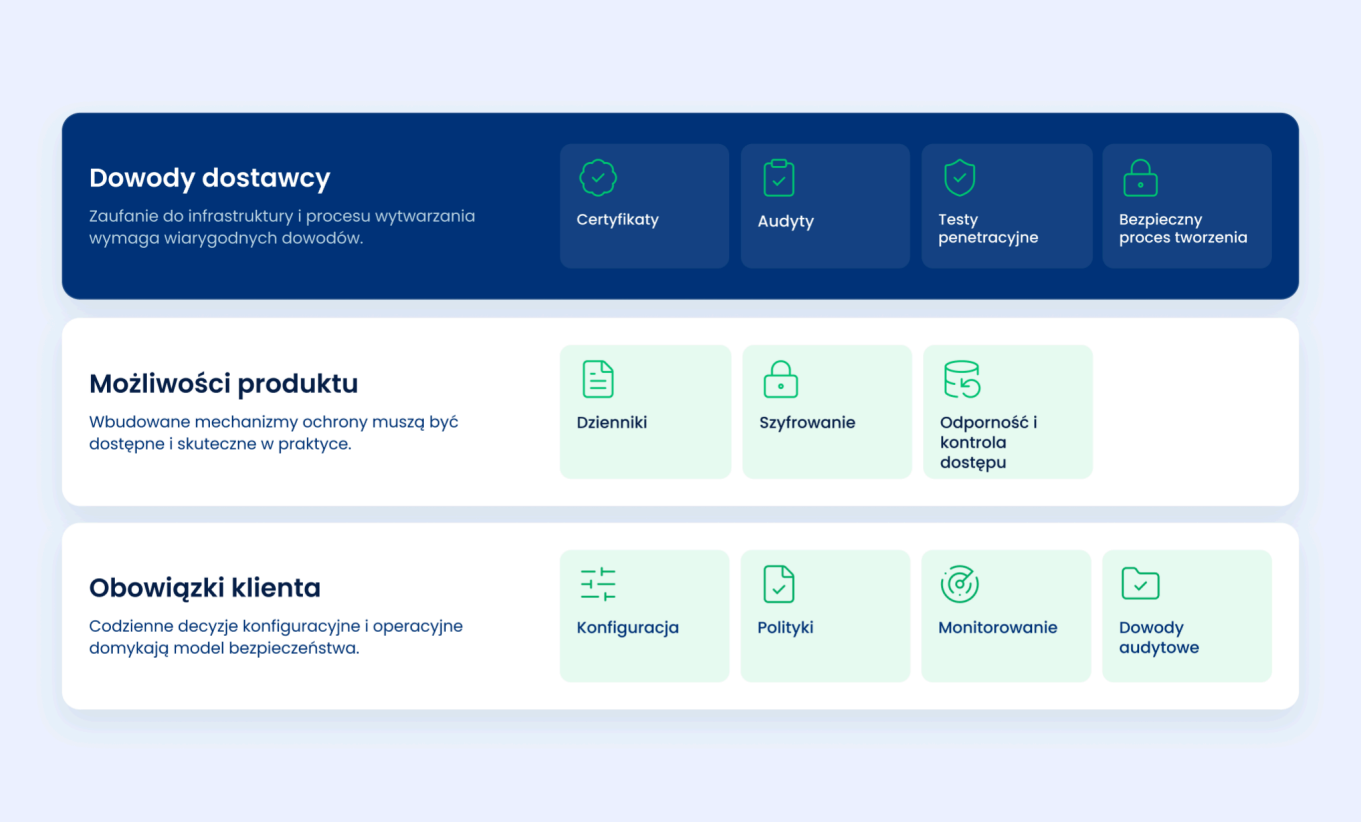
- System zarządzania bezpieczeństwem informacji
- Bezpieczny cykl życia tworzenia oprogramowania
- Proces przeglądu kodu źródłowego i zależności
- Wewnętrzne i zewnętrzne testy penetracyjne
- Proces zgłaszania i usuwania podatności
- Procedury powiadamiania klientów
- Szyfrowanie danych podczas przesyłania i przechowywania
- Zarządzanie kluczami
- Przechowywanie i usuwanie danych
- Tworzenie kopii zapasowych i odzyskiwanie danych
- Ciągłość działania

Sama lokalizacja danych nie stanowi potwierdzenia zgodności. Należy przeanalizować lokalizacje przetwarzania danych, podmioty podprzetwarzające (ang. *subprocessors*), transfery międzynarodowe, dostęp personelu pomocy technicznej, zabezpieczenia kontraktowe oraz warunki powiadamiania o naruszeniach.

Odpowiednie wymagania, przepisy, normy i wytyczne mogą obejmować RODO, dyrektywę NIS2, ustawę o krajowym systemie cyberbezpieczeństwa (KSC), rozporządzenie DORA, standard PCI

© 2026 Rublon

DSS, ustawę HIPAA, przepisy FTC Safeguards Rule, wytyczne instytutu NIST, warunki ubezpieczenia cybernetycznego oraz inne przepisy dotyczące zgodności i stosowne obowiązki.



Skuteczne zapewnienie bezpieczeństwa MFA zależy od dowodów po stronie dostawcy, możliwości produktu i właściwych działań po stronie klienta.

7.3. Ocena nie tylko produktu, ale i dostawcy

Z platformy MFA korzysta się przez lata, podczas gdy aplikacje, systemy operacyjne, standardy i zagrożenia ciągle się zmieniają.

Należy ocenić specjalizację dostawcy w zakresie uwierzytelniania MFA i bezpieczeństwa tożsamości, historię ostatnich wydań, plan rozwoju produktu oraz zdolność do wyjaśniania zagrożeń związanych z integracją i odzyskiwaniem dostępu.

Podczas okresu próbnego należy przetestować pomoc techniczną, zadając reprezentatywne pytania techniczne. Należy ocenić czas odpowiedzi, poprawność informacji, możliwości eskalacji, obsługiwane języki i strefy czasowe oraz to, czy pomoc techniczna jest świadczona bezpośrednio, czy za pośrednictwem pośredników.

Dokumentacja powinna być aktualna, wersjonowana i szczegółowa oraz w przejrzysty sposób przedstawiać wymagania wstępne i ograniczenia.

© 2026 Rublon

Referencje klientów są najbardziej przydatne, gdy dotyczą wdrożeń podobnych do planowanego. Należy zapytać o nakład pracy związany z wdrożeniem, doświadczenia z aktualizacjami, nieoczekiwane ograniczenia, wpływ na dział pomocy technicznej oraz wsparcie po sprzedaży.

Ekosystem partnerów może zapewniać lokalną wiedzę specjalistyczną, ale odpowiedzialność za błędy, zgodność, eskalację i długoterminowe wsparcie musi być jasno określona.

Dostawcy działający w sposób przejrzysty dokumentują nieobsługiwane scenariusze, ograniczenia architektoniczne i incydenty. Miarodajny okres próbny powinien obejmować reprezentatywne integracje, funkcjonalność zbliżoną do środowiska produkcyjnego oraz pomoc techniczną.

8. Przeprowadzenie miarodajnej weryfikacji koncepcji

8.1. Opracowanie planu weryfikacji koncepcji rozwiązania MFA

Weryfikacja koncepcji (ang. *proof of concept*) powinna obejmować testowanie warunków, które mogą wpłynąć na decyzję zakupową. Nie powinna ograniczać się do dopracowanej demonstracji ani aplikacji najłatwiejszej do zabezpieczenia.

Należy określić objęte zakresem systemy, grupy użytkowników, źródła tożsamości, metody, polityki i scenariusze awarii. Trzeba wyznaczyć osoby odpowiedzialne z zespołów ds. bezpieczeństwa, infrastruktury, zarządzania tożsamością i dostępem (IAM), pomocy technicznej oraz aplikacji.

8.1.1. Określenie kryteriów powodzenia

Należy sprawdzić, czy:

- Wymagane aplikacje są chronione za pośrednictwem przewidzianych dla nich ścieżek dostępu
- Użytkownicy i grupy są prawidłowo synchronizowane
- Wymagane metody działają z każdą integracją
- Czas uwierzytelniania jest akceptowalny
- Polityki zapewniają oczekiwane rezultaty
- Dzienniki zawierają wystarczający kontekst
- Proces odzyskiwania dostępu zachowuje odpowiedni poziom pewności co do tożsamości

© 2026 Rublon

- Mechanizmy wysokiej dostępności i przełączania awaryjnego działają prawidłowo
- Nakład pracy administracyjnej jest możliwy do utrzymania
- Opinie użytkowników i działu pomocy technicznej są akceptowalne

Należy rejestrować czas potrzebny na skonfigurowanie integracji, przypisanie polityki, zarejestrowanie użytkowników, wymianę uwierzytelniacza, zdiagnozowanie błędu i unieważnienie dostępu.

8.1.2. Zastosowanie reprezentatywnych scenariuszy

Należy uwzględnić:

- Pracownika biurowego
- Użytkownika zdalnego korzystającego z sieci VPN
- Administratora
- Wykonawcę
- Użytkownika bez smartfona
- Użytkownika korzystającego z klucza sprzętowego lub klucza dostępu FIDO2
- Użytkownika wymieniającego telefon
- Użytkownika z ograniczoną łącznością
- Nieuprawnionego użytkownika
- Awarię konektora lub usługi katalogowej

Należy przetestować zarówno pomyślne, jak i nieudane ścieżki. Trzeba odrzucać żądania i doprowadzać do ich wygaśnięcia. Należy wyłączać konta, usuwać użytkowników z grup, unieważniać uwierzytelniacze, a następnie ponownie podejmować próby uzyskania dostępu.

Należy prześledzić pełny proces odzyskiwania dostępu, od zgłoszenia utraty urządzenia przez weryfikację, dostęp tymczasowy, ponowną rejestrację i powiadomienie aż po unieważnienie uwierzytelniacza.

8.1.3. Gromadzenie dowodów

Należy zgromadzić:

- Zrzuty ekranu konfiguracji i monitów
- Dzienniki uwierzytelniania i dzienniki audytowe
- Czas wdrożenia
- Zmiany w konfiguracji zapory sieciowej
- Komponenty lokalne
- Konta usługowe i certyfikaty

© 2026 Rublon

- Zależności zewnętrzne
- Czynności wykonywane ręcznie i pliki konfiguracyjne
- Opinie użytkowników i administratorów
- Jakość odpowiedzi pomocy technicznej
- Znane ograniczenia i sposoby obejścia problemów

Wynik końcowy powinien przedstawiać wymagania dotyczące wdrożenia produkcyjnego, w tym nierozstrzygnięte założenia i konieczne kompromisy.

8.2. Karta oceny dostawcy rozwiązania MFA

Karta oceny przekształca deklaracje dostawców i wyniki weryfikacji koncepcji w porównywalny zapis procesu decyzyjnego. Kategorie i ich wagi należy uzgodnić przed analizą ostatecznych ofert.

Wagi mogą różnić się w zależności od środowiska. Organizacje z sektora opieki zdrowotnej mogą traktować priorytetowo dostępność i dostęp awaryjny. Instytucje finansowe mogą przywiązywać większą wagę do odporności na phishing i możliwości audytowych. Środowiska z dużą liczbą systemów starszego typu mogą przypisywać większą wagę zakresowi integracji.

Kategoria oceny	Sugerowana waga
Skuteczność zabezpieczeń	20%
Zakres integracji	20%
Metody uwierzytelniania	10%
Wdrożenie i eksploatacja	15%
Doświadczenie użytkownika	10%
Administracja i raportowanie	10%
Niezawodność i wiarygodność dostawcy	10%
Całkowity koszt posiadania	5%
Razem	**100%**

Należy stosować jedną skalę punktową:

© 2026 Rublon

Wynik	Znaczenie
0	Brak obsługi
1	Poważna luka lub niepraktyczny sposób obejścia problemu
2	Częściowa obsługa z istotnymi ograniczeniami
3	Spełnia wymaganie
4	Przewyższa wymaganie
5	Znacznie przewyższa wymaganie, co potwierdzają zweryfikowane dowody

Wymagania obowiązkowe muszą być oddzielone od wyniku całkowitego. Dobre wyniki w kategoriach niskiego ryzyka nie powinny rekompensować braku krytycznej integracji, metody lub mechanizmu zapewniającego odporność.

8.3. Arkusz oceny dostawcy

Wszelkie zapewnienia dostawcy traktuj wyłącznie jako deklaracje, dopóki nie znajdą potwierdzenia w dokumentacji, umowie lub udanych testach. Ograniczenia należy rejestrować nawet w przypadku pozytywnej weryfikacji wymogu.

Wymaganie	Priorytet	Odpowiedź dostawcy	Przedstawione dowody	Wynik weryfikacji koncepcji	Wynik	Uwagi	Zidentyfikowane ograniczenia
	Obowiązkowy / Wysoki / Średni / Niski		**Dokumentacja / demonstracja / umowa / test**	**Spełnione / Częściowo spełnione / Niespełnione / Nieprzetestowane**	**0-5**		

© 2026 Rublon

8.4. Sygnały ostrzegawcze podczas oceny dostawcy MFA

Sygnały ostrzegawcze należy zidentyfikować, zanim platforma stanie się krytyczną zależnością.

Należy zachować ostrożność, gdy:

- Demonstrowane są wyłącznie aplikacje chmurowe
- Sieci VPN, systemy Windows, systemy Linux, urządzenia sieciowe lub systemy starszego typu są wyłączone z zakresu ochrony
- Funkcje znacznie różnią się między integracjami, a różnice te nie są jasno przedstawione
- Ważne funkcjonalności wymagają nieoczekiwanych modułów, licencji lub usług
- Funkcjonalność wersji próbnej znacząco różni się od funkcjonalności dostępnej w ramach licencji produkcyjnej
- Nie można wyjaśnić zachowania podczas awarii, przełączania awaryjnego i odzyskiwania
- Nie jest dostępna żadna metoda odporna na phishing
- Obsługa środowisk lokalnych i systemów typu legacy jest ograniczona
- Dzienniki nie umożliwiają rozróżnienia odrzucenia, przekroczenia limitu czasu, odmowy wynikającej z polityki i błędu technicznego
- Działania administracyjne i zmiany uwierzytelniaczy nie podlegają audytowi
- Proces wymiany urządzenia nie obejmuje wiarygodnej weryfikacji tożsamości
- Przepływy danych, lokalizacje przetwarzania i podmioty podprzetwarzające nie są jasno określone
- Ograniczenia i restrykcje dotyczące wersji nie są udokumentowane
- Z weryfikacji koncepcji wyłączone są trudne scenariusze

Dopracowany proces logowania w przeglądarce nie potwierdza zakresu ochrony obejmującego całe przedsiębiorstwo. Dostawca, który działa w sposób przejrzysty, powinien przed wdrożeniem wyjaśnić ograniczenia architektoniczne, różnice między metodami, zależności i zachowanie procesu odzyskiwania.

9. Jak rozwiązanie Rublon MFA spełnia kryteria oceny?

9.1. Najważniejsze informacje o rozwiązaniu Rublon MFA

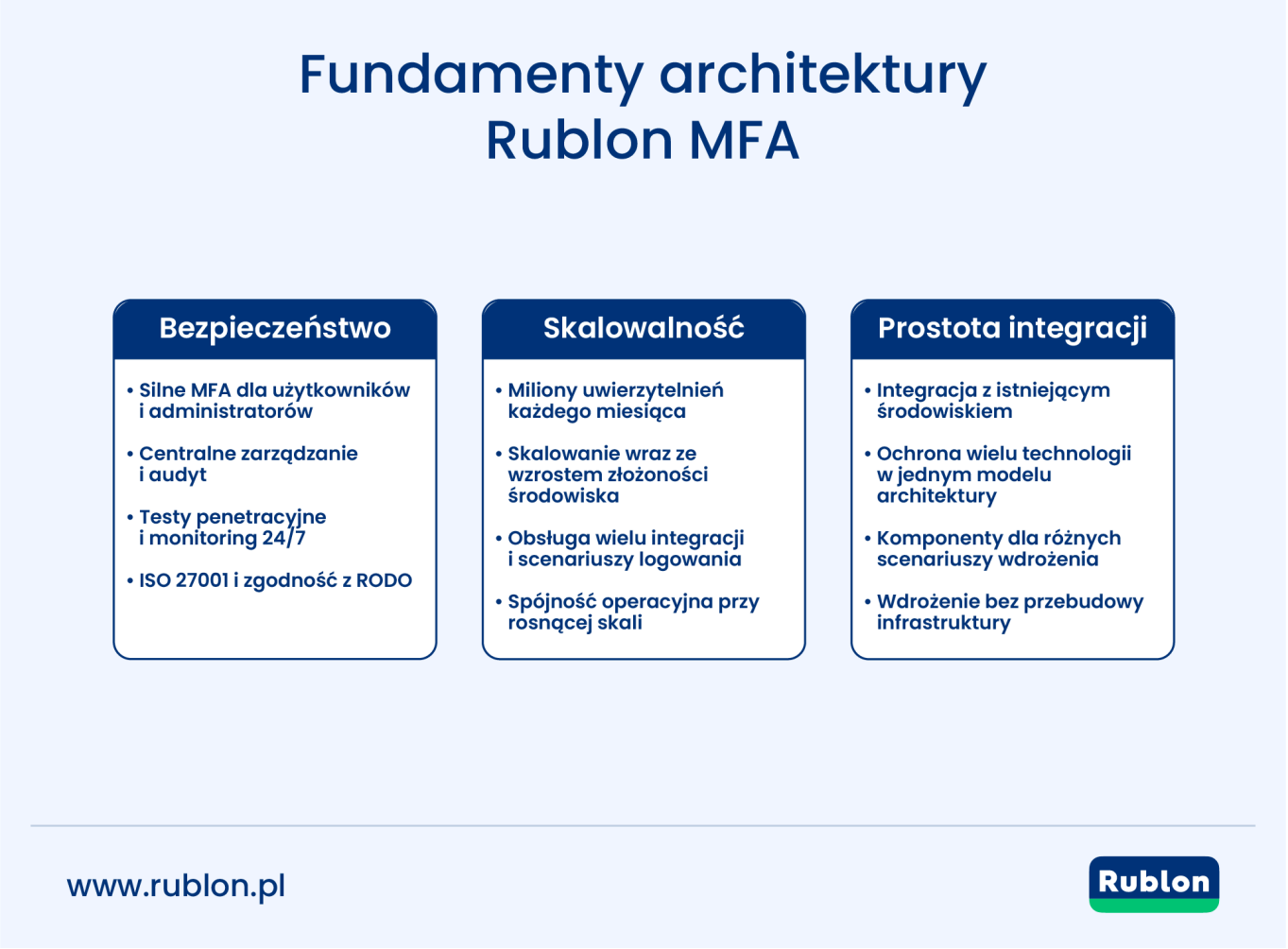
Rozwiązanie Rublon MFA to centralnie zarządzana platforma uwierzytelniania MFA dla przedsiębiorstw, przeznaczona do środowisk chmurowych, lokalnych i hybrydowych. Dodaje uwierzytelnianie wieloskładnikowe do istniejącej infrastruktury tożsamości i uwierzytelniania

© 2026 Rublon

bez konieczności zastępowania używanych przez organizację usług katalogowych, dostawców tożsamości ani procesów logowania.

Konsola Rublon Admin Console centralizuje zarządzanie użytkownikami, aplikacjami, grupami, politykami, uwierzytelniaczami, zapamiętanymi urządzeniami, dziennikami i działaniami administracyjnymi.

Architektura rozwiązania Rublon MFA obsługuje nowoczesne aplikacje, umożliwiając jednocześnie zachowanie systemów opartych na usłudze Active Directory, usłudze Microsoft Entra ID, protokole LDAP, protokole RADIUS, standardzie SAML oraz procesach logowania specyficznych dla poszczególnych aplikacji. Organizacje mogą stopniowo rozszerzać zakres ochrony zgodnie z poziomem ryzyka i priorytetami modernizacji.



9.2. Ochrona krytycznych ścieżek dostępu w organizacji

Rozwiązanie Rublon MFA stosuje uwierzytelnianie w miejscu, w którym użytkownicy uzyskują dostęp do systemów.

- Rublon Authentication Proxy działa jako lokalny serwer proxy korzystający z protokołu RADIUS lub LDAP dla zgodnych sieci VPN, zapór sieciowych, urządzeń sieciowych i usług dostępu. Może łączyć się ze źródłami tożsamości, takimi jak usługa Active Directory, usługa Microsoft Entra ID, usługa katalogowa OpenLDAP, system FreeIPA, serwer FreeRADIUS i usługa Microsoft NPS. Kilka instancji usługi Rublon Authentication Proxy może zapewniać wysoką dostępność.
- Rublon MFA dla Windows Logon i RDP chroni obsługiwane lokalne logowania do systemu Windows oraz sesje korzystające z protokołu Remote Desktop Protocol.
- Zakres ochrony usługi Remote Desktop Services obejmuje bramę Remote Desktop Gateway, usługę Remote Desktop Web Access, klienta RD Web Client oraz kanał RD Web Feed. Uwierzytelnianie MFA można stosować na poziomie bramy, warstwy dostępu internetowego, hosta sesji lub w kilku punktach ścieżki dostępu.
- Rublon MFA dla Linux SSH korzysta z modułów PAM i chroni obsługiwane lokalne oraz zdalne uwierzytelnianie za pomocą protokołu SSH, w tym dostęp oparty na haśle i skonfigurowane scenariusze wykorzystujące klucze SSH.
- Rublon MFA dla macOS integruje się z mechanizmem logowania systemu macOS i chroni logowania dodając drugi krok uwierzytelniania po zweryfikowaniu hasła użytkownika.
- Rublon Access Gateway zapewnia integrację ze standardem SAML 2.0 dla aplikacji chmurowych i federacyjnych.
- Rublon Identity Bridge obsługuje aplikacje oparte na protokołach OAuth 2.0 i OpenID Connect za pośrednictwem scentralizowanej warstwy autoryzacji.
- Rublon App Shield chroni samodzielnie hostowane aplikacje internetowe bez konieczności zmieniania ich kodu źródłowego. Może obejmować ochroną portale wewnętrzne, panele administracyjne, starsze systemy internetowe oraz inne aplikacje obsługiwane w przeglądarce.
- Rublon MFA dla AD FS dodaje MFA do usługi Active Directory Federation Services, chroniąc federacyjny dostęp do aplikacji i usług korzystających z AD FS.
- Rublon MFA dla Outlook Web App (OWA) dodaje MFA do logowania do Outlook Web App oraz Exchange Control Panel w obsługiwanych środowiskach Microsoft Exchange.
- Rublon MFA dla Roundcube dodaje MFA do logowania do poczty internetowej Roundcube za pomocą dedykowanego konektora, wymagając dodatkowej metody uwierzytelniania po podaniu danych logowania.
- Rublon REST API i biblioteki Rublon SDK umożliwiają dodanie uwierzytelniania MFA do aplikacji opracowanych wewnętrznie, w tym przepływów z interfejsem graficznym i bez monitów.
- Dostępność metod uwierzytelniania i wygoda użytkownika różnią się w zależności od integracji, dlatego każdą krytyczną ścieżkę należy zweryfikować na podstawie aktualnej dokumentacji i testów przeprowadzonych w ramach weryfikacji koncepcji.

© 2026 Rublon

9.3. Metody uwierzytelniania dla różnych użytkowników i poziomów ryzyka

Rozwiązanie Rublon MFA obsługuje metody programowe i sprzętowe przeznaczone dla różnych użytkowników, aplikacji i poziomów ryzyka. Polityka Metody uwierzytelniania określa, które metody są dostępne dla aplikacji i grup.

Aplikacja mobilna Rublon Authenticator obsługuje:

- Powiadomienie mobilne
- Kod dostępu oparty na algorytmie TOTP (RFC 6238), działający bez połączenia z Internetem
- Uwierzytelnianie za pomocą kodu QR
- Rejestrację na wielu urządzeniach mobilnych

W przypadku dostępu o podwyższonym poziomie ryzyka rozwiązanie Rublon MFA obsługuje klucze bezpieczeństwa FIDO U2F i FIDO2, a także klucze dostępu zgodne ze standardem FIDO2, przechowywane za pomocą funkcji Windows Hello, zgodnych menedżerów haseł, urządzeń mobilnych lub kluczy fizycznych.

Zgodne aplikacje innych firm, w tym Google Authenticator i Microsoft Authenticator, generują kody dostępu TOTP. Metoda Kod dostępu obsługuje również sprzętowe tokeny OATH korzystające z algorytmu SHA-1. Metoda YubiKey OTP zapewnia kolejną opcję sprzętową, ale w przeciwieństwie do standardu FIDO2 nie jest odporna na phishing.

Metody Kod SMS i Połączenie telefoniczne mogą być odpowiednie dla użytkowników, którzy nie są w stanie skorzystać z aplikacji uwierzytelniającej lub nie mają niezawodnego połączenia z Internetem. Metody Link SMS i Link e-mail stanowią dodatkowe alternatywy, ale wymagają dostępu do sieci w celu otwarcia linku weryfikacyjnego. Metody Kod SMS, Link SMS i Połączenie telefoniczne zużywają kredyty telefoniczne i zasadniczo lepiej sprawdzają się jako metody zapewniające dostępność, wspierające okres przejściowy lub odzyskiwanie dostępu niż w przypadku dostępu uprzywilejowanego.

Obsługiwane wdrożenia Rublon MFA dla Windows Logon i RDP mogą również korzystać z kart RFID, identyfikatorów, breloków i innych uwierzytelniaczy wykorzystujących technologię RFID.

Proces odzyskiwania dostępu może łączyć uwierzytelniacze zapasowe z kodami pominięcia wydawanymi przez administratora, które mają konfigurowalny termin ważności i limit użycia.

© 2026 Rublon

9.4. Scentralizowane polityki, administracja i widoczność

Konsola Rublon Admin Console centralizuje zarządzanie aplikacjami, użytkownikami, grupami, politykami, uwierzytelniaczami, zapamiętanymi urządzeniami, synchronizacją usług katalogowych, dostępem administracyjnym i raportowaniem.

Role administratorów umożliwiają pracownikom pomocy technicznej wykonywanie wybranych zadań związanych z odzyskiwaniem dostępu i uwierzytelniaczami bez przyznawania im pełnego dostępu do polityk czy rozliczeń.

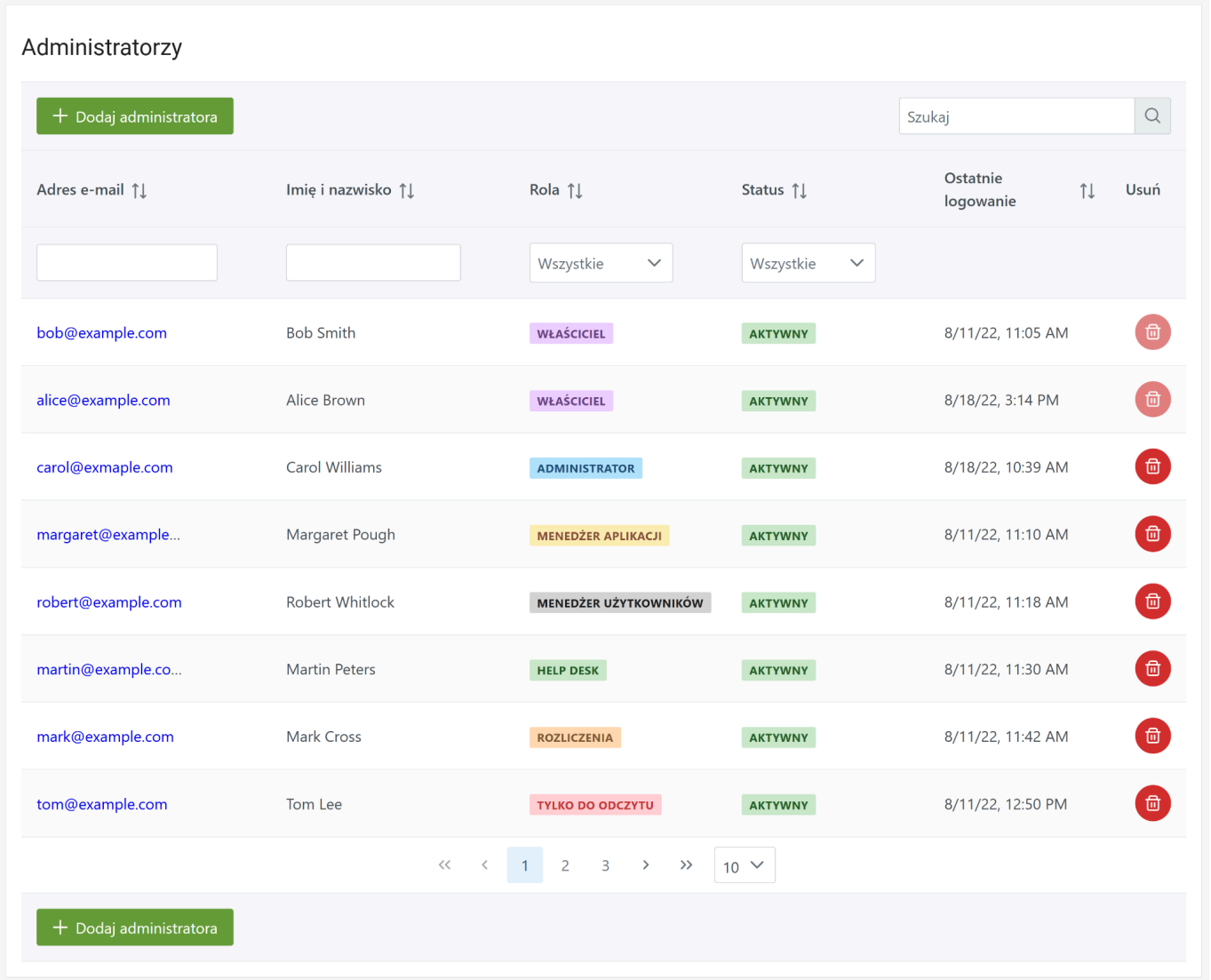
Funkcja Directory Sync importuje użytkowników i grupy z usługi Microsoft Entra ID. Synchronizacja z usługą Active Directory i usługą katalogową OpenLDAP jest dostępna za pośrednictwem usługi Rublon Authentication Proxy.

Rejestry operacyjne obejmują:

- **Dzienniki uwierzytelniania:** użytkownik, aplikacja, urządzenie, metoda, wynik, czas, adres IP, przeglądarka, system operacyjny oraz dostępne dane o lokalizacji
- **Dzienniki aktywności:** zmiany uwierzytelniaczy wprowadzone za pośrednictwem procesów samoobsługowych
- **Dzienniki audytowe:** działania administracyjne
- **Dzienniki telefoniczne:** stan dostarczenia i wykorzystanie kredytów telefonicznych

Rozwiązanie Rublon Log Sync potrafi w sposób ciągły pobierać te dzienniki z interfejsu Rublon Admin API i przekazywać je do zgodnego systemu SIEM na potrzeby scentralizowanego monitorowania i analizy.

Zapamiętane urządzenia są widoczne centralnie i podlegają politykom. Można ograniczyć lub wyłączyć ich używanie w przypadku użytkowników uprzywilejowanych i aplikacji krytycznych.



9.5. Wdrożenie w istniejącej infrastrukturze

Rozwiązanie Rublon MFA dodaje uwierzytelnianie do istniejących środowisk bez zastępowania ich podstawowej infrastruktury tożsamości.

Obsługuje tożsamości pochodzące z usługi Active Directory, usługi Microsoft Entra ID oraz zgodnych usług katalogowych korzystających z protokołu LDAP. Synchronizacja katalogów importuje użytkowników i grupy na potrzeby przypisywania aplikacji i egzekwowania polityk.

Systemy korzystające z protokołów RADIUS i LDAP można integrować za pośrednictwem usługi Rublon Authentication Proxy. Aplikacje korzystające ze standardu SAML mogą używać aplikacji Rublon Access Gateway. Dedykowane konektory obejmują logowanie do systemu Windows, usługi Remote Desktop Services, dostęp do systemu Linux za pomocą protokołu SSH, usługi firmy Microsoft oraz wybrane aplikacje chmurowe.

© 2026 Rublon

Systemy bez natywnego konektora mogą korzystać z protokołów ogólnego przeznaczenia, rozwiązania Rublon App Shield, rozwiązania Rublon Identity Bridge, interfejsu Rublon REST API lub bibliotek Rublon SDK.

Dokumentacja poszczególnych aplikacji opisuje wymagania wstępne, konfigurację, przepływy uwierzytelniania oraz istotne ograniczenia.

Etapowe wdrożenie można rozpocząć od środowiska przedprodukcyjnego i niewielkiego programu pilotażowego. Zespoły mogą zweryfikować rejestrację, polityki, metody, błędy, dzienniki i procedury pomocy technicznej przed rozpoczęciem egzekwowania zabezpieczeń na większą skalę.

Wdrożenie może przebiegać według grup, aplikacji lub ścieżek dostępu. W pierwszej kolejności można objąć ochroną administratorów i dostęp za pośrednictwem sieci VPN, a następnie serwery, usługi chmurowe, aplikacje internetowe, systemy używane przez pracowników oraz bardziej złożone aplikacje starszego typu.

Pozwala to utrzymywać nowoczesne i starsze systemy w ramach jednej platformy MFA, podczas gdy modernizacja przebiega w możliwym do zarządzania tempie.

Więcej informacji: Poradnik Rublon dotyczący najlepszych praktyk wdrożeniowych.

9.6. Korzyści operacyjne i kwestie dotyczące całkowitego kosztu

Rozwiązanie Rublon MFA korzysta z subskrypcji rozliczanych za użytkownika. Opublikowany cennik obejmuje nieograniczoną liczbę integracji z aplikacjami. Dodanie kolejnej obsługiwanej sieci VPN, serwera, usługi chmurowej lub aplikacji internetowej nie powoduje naliczenia oddzielnej opłaty za integrację z aplikacją.

Metody Kod SMS, Link SMS i Połączenie telefoniczne zużywają kupowane oddzielnie kredyty telefoniczne. Wykorzystanie należy oszacować na podstawie liczby użytkowników, częstotliwości użycia, kraju docelowego oraz potrzeb związanych z odzyskiwaniem dostępu.

Niektóre integracje wymagają hostów zarządzanych przez klienta, certyfikatów, monitorowania, aktualizacji oraz rozwiązań zapewniających wysoką dostępność. W całkowitym koszcie posiadania należy również uwzględnić nakład pracy wewnętrznych zespołów technicznych i działu pomocy technicznej.

Nieograniczona liczba obsługiwanych integracji z aplikacjami umożliwia rozszerzanie platformy bez konieczności zakupu nowej kategorii licencji dla każdego zasobu. Konsolidacja oddzielnych narzędzi MFA może również obniżyć koszty, w zależności od warunków umów, nakładu pracy związanego z migracją oraz wymagań technicznych.

© 2026 Rublon

9.7. Pomoc techniczna, dokumentacja i zapewnienie bezpieczeństwa

Spółka Rublon udostępnia dokumentację techniczną, poradniki dotyczące integracji, pliki do pobrania, materiały dotyczące architektury, informacje o wydaniach, wskazówki dotyczące wdrażania oraz materiały wspierające komunikację z użytkownikami.

Zespół Rublon Support pomaga klientom w języku angielskim, niemieckim i polskim. Aktualne informacje o działaniu usług są dostępne na stronie stanu Rublon.

Trzydziestodniowa wersja próbna rozwiązania Rublon MFA zapewnia dostęp do funkcji platformy bez konieczności podawania danych karty płatniczej, dzięki czemu organizacje mogą przetestować reprezentatywne integracje i procesy.

Spółka Rublon stosuje certyfikowany system zarządzania bezpieczeństwem informacji zgodny z normą PN-EN ISO/IEC 27001:2023. Dokumentacja dotycząca bezpieczeństwa i kwestii prawnych obejmuje ochronę danych, prywatność, warunki przetwarzania oraz informacje o podmiotach podprzetwarzających. Umowa o gwarantowanym poziomie świadczenia usług Rublon zobowiązuje dostawcę do zapewnienia miesięcznej dostępności na poziomie co najmniej 99,9% w przypadku objętego umową płatnego korzystania z usługi, z uwzględnieniem określonych w niej warunków i wyłączeń.

Historie klientów i niezależne recenzje stanowią dodatkowe źródło informacji o wdrożeniu, łatwości użytkowania i jakości pomocy technicznej w różnych branżach.

10. Podsumowanie i materiały dla kupujących

10.1. Końcowa lista kontrolna dla kupującego rozwiązanie MFA

10.1.1. Zakres i ochrona

☐ Przeprowadzono inwentaryzację aplikacji, systemów i ścieżek dostępu.

☐ Zidentyfikowano tożsamości pracowników, administratorów, wykonawców, partnerów i użytkowników zewnętrznych.

☐ Konta uprzywilejowane i awaryjne sklasyfikowano oddzielnie.

☐ Uwzględniono dostęp chmurowy, lokalny, zdalny i hybrydowy.

☐ Oceniono aplikacje typu legacy i aplikacje niestandardowe.

☐ Udokumentowano systemy, które nadal korzystają wyłącznie z haseł, oraz zaakceptowano związane z nimi ryzyko.

10.1.2. Uwierzytelnianie i polityki

☐ Wymagane metody działają za pośrednictwem przewidzianych integracji.

☐ Klucze bezpieczeństwa lub klucze dostępu zgodne ze standardem FIDO2 przetestowano w przypadku dostępu wysokiego ryzyka.

☐ Zweryfikowano polityki dotyczące użytkowników, administratorów, wykonawców i kont awaryjnych.

☐ Słabsze metody zapasowe nie mogą bez autoryzacji omijać silniejszych wymagań.

☐ Polityki dotyczące zapamiętanych urządzeń, sieci, lokalizacji i odzyskiwania dostępu działają zgodnie z oczekiwaniami.

☐ Przetestowano mechanizmy rejestracji, wymiany i ponownej rejestracji uwierzytelniaczy.

10.1.3. Eksploatacja i odporność

☐ Dzienniki uwierzytelniania i dzienniki audytu zapewniają wystarczający kontekst.

☐ Potwierdzono wymagania dotyczące przechowywania, eksportowania i przekazywania danych do platformy SIEM.

☐ Uprawnienia działu pomocy technicznej są zgodne z zasadą najmniejszych uprawnień.

☐ W wymaganych przypadkach przetestowano scenariusze działania w trybie offline i przy ograniczonej łączności.

☐ Udokumentowano zachowanie podczas awarii konektora, usługi katalogowej, sieci i usługi chmurowej.

☐ Zatwierdzono decyzje dotyczące trybu fail-open i trybu fail-closed.

☐ Przetestowano mechanizmy wysokiej dostępności i odzyskiwania konfiguracji.

☐ Przypisano odpowiedzialność za monitorowanie, utrzymanie i aktualizacje.

© 2026 Rublon

10.1.4. Ocena warunków handlowych i dostawcy

☐ Spójnie obliczono trzyletni całkowity koszt posiadania.

☐ Uwzględniono koszty subskrypcji, wykorzystania, sprzętu, infrastruktury, pomocy technicznej i pracy personelu.

☐ Uwzględniono przewidywany wzrost liczby użytkowników i aplikacji.

☐ Przeanalizowano certyfikacje, dokumenty dotyczące prywatności, informacje o podmiotach podprzetwarzających i zobowiązania dotyczące świadczenia usług.

☐ Przetestowano pomoc techniczną za pomocą reprezentatywnych pytań.

☐ Referencje klientów odpowiadają planowanemu wdrożeniu.

☐ Zarejestrowano ograniczenia, sposoby obejścia problemów i nieobsługiwane scenariusze.

☐ Porównano funkcjonalność wersji próbnej z zakresem licencji produkcyjnej.

10.1.5. Gotowość do wdrożenia

☐ Spełniono obowiązkowe wymagania dotyczące weryfikacji koncepcji.

☐ Przeanalizowano opinie użytkowników i administratorów.

☐ Określono przewidywany wpływ na dział pomocy technicznej.

☐ Wybrano użytkowników i aplikacje do programu pilotażowego.

☐ Przygotowano plany komunikacji, szkoleń, eskalacji i wycofania zmian.

☐ Określono mierniki powodzenia i sposób raportowania poziomu wdrożenia.

☐ Zatwierdzono etapowy plan wdrożenia.

10.2. Następne kroki

Zweryfikuj rozwiązanie Rublon MFA w odniesieniu do tożsamości, aplikacji i ścieżek dostępu istotnych dla Twojej organizacji.

Skorzystaj z 30-dniowego okresu próbnego, aby połączyć reprezentatywne systemy, przetestować wymagane metody i polityki, przeanalizować dzienniki oraz przeprowadzić scenariusze odzyskiwania dostępu i awarii. Zapoznaj się z dokumentacją integracji dotyczącą

© 2026 Rublon

sieci VPN, systemów Windows i Linux, usługi Remote Desktop Services, usług chmurowych, aplikacji internetowych i pozostałej infrastruktury.

W przypadku nieobsługiwanych lub niestandardowych aplikacji skontaktuj się z Rublon, aby omówić architekturę uwierzytelniania i dostępne opcje integracji. Konsultacja dotycząca architektury może również pomóc w określeniu komponentów lokalnych, połączeń z usługami katalogowymi, wymagań dotyczących odporności, zakresu weryfikacji koncepcji oraz kolejności wdrożenia.

Rozpocznij ocenę rozwiązania Rublon MFA w rzeczywistym środowisku dostępu swojej organizacji:

- Rozpocznij bezpłatny okres próbny
- Sprawdź obsługiwane integracje
- Skontaktuj się z Rublon

Rublon sp. z o.o.
ul. Stanisława Wyspiańskiego 11
65-036 Zielona Góra

www.rublon.pl

© 2026 Rublon sp. z o.o.