SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Spis treści

A. Przedmiot zamówienia

W ramach realizacji przedmiotu zamówienia mieści się:

1. Dostawa licencji brokera zabezpieczeń dostępu do aplikacji w chmurze – w terminie nie dłuższym niż 14 dni kalendarzowych od daty podpisania umowy.
2. Świadczenie serwisu i wsparcia technicznego Producenta przez okres minimum 24 miesięcy, licząc od daty podpisania bez uwag protokołu odbioru.

B. Wymagania dotyczące dostawy sprzętu, oprogramowania oraz licencji

1. Koszty dostawy (w tym koszty opakowania, ubezpieczenia, transportu) ponosi Wykonawca
2. Licencja musi być nowa, wcześniej nieużywana.
3. Wykonawca zobowiązuje się dostarczyć wymagane oprogramowanie oraz licencje pochodzące z legalnego źródła, fabrycznie nowe, zakupione w autoryzowanym kanale sprzedaży producenta i objęte standardowym pakietem usług gwarancyjnych świadczonych przez sieć serwisową producenta na terenie Polski.
4. Dostarczone do Zamawiającego licencje muszą być w postaci wygenerowanych na stronie producenta plików licencyjnych lub w formie wygenerowanych i przesłanych emailem przez Wykonawcę plików na adres email wskazany przez Zamawiającego (sbt@ncbr.gov.pl).

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

C. Wymagania dotyczące zakresu usług

1. Wymagania dot. świadczenie wsparcia technicznego i serwisu Producenta zostały szczegółowo opisane w minimalnych wymaganiach poszczególnych urządzeń i oprogramowania.
2. Wymagania dot. gwarancji Producenta zostały szczegółowo opisane w minimalnych wymaganiach oprogramowania

D. Opis istniejącego środowiska

1. Zamawiający korzysta aktywnie z oprogramowania Office 365, w wersji E5 dla 950 użytkowników.
2. Zamawiający posiada i wykorzystuje IdP w postaci ADFS.
3. Zamawiający wykorzystuje jako bramka sieciowa urządzenia Fortigate oraz Palo Alto.
4. Zamawiający wykorzystuje Azure Information Protection do klasyfikacji danych.
5. Zamawiający wykorzystuje oprogramowanie SIEM – Splunk Enterprise

E. Wymagania funkcjonalne dla centralnie zarządzanego oprogramowania do zabezpieczenia serwerów fizycznych, wirtualnych i w chmurze

LP	Cecha	Wymagalne minimalne parametry techniczne
	Wymagania ogólne	1. Zapewnienie pełnej funkcjonalności niezależnie od urządzenia, typu klienta i lokalizacji. CASB musi zapewnić pełną funkcjonalność opartą na polityce dla każdej "zaufanej", "niezaufanej" lub "nie w pełni zaufanej" aplikacji, niezależnie od tego, czy dostęp do niej jest z komputera stacjonarnego, laptopa, czy urządzenia mobilnego w siedzibie firmy lub zdalnie, niezależnie od klienta (przeglądarka, aplikacja natywna, synchronizacja itp.). 2. Rozwiązanie CASB musi obsługiwać tryby: ○ API ○ Proxy ○ Log Collection 3. Rozwiązanie CASB musi obsługiwać (ale nie tylko) wymienione poniżej aplikacje w trybie API i Proxy: ○ Office 365 ○ Jira Cloud 4. Wszystkie dane w tranzycie, które obejmują dane

		przepływające przez lub pomiędzy systemem CASB, użytkownikami końcowymi, a istniejącymi systemami Zamawiającego (on-premise lub cloud takimi jak IAM, SIEM) muszą być szyfrowane. 5. Rozwiązanie CASB musi zapewniać różne poziomy kontroli dostępu w oparciu o RBAC tj. zapewnić elastyczny dostęp do danych i możliwości produktu w oparciu o rolę przypisaną użytkownikowi przez administratora CASB 6. Zapewnienie logów audytowych zmian dla zarządzania konfiguracją i kontroli zmian. CASB musi zapewnić logi audytu dla zmian polityki i konfiguracji dokonanych przez administratora. 7. Wsparcie standardowych typów logów dla integracji z usługami identyfikacyjnymi. CASB musi zapewniać możliwość odczytu szeregu logów z bramy internetowej i firewalla w różnych formatach, w tym między innymi CEF, CLSF i syslog. 8. Integracja z korporacyjnym proxy lub bramą internetową. Kiedy CASB działa w trybie proxy musi być w stanie zintegrować się z każdą istniejącą bezpieczną bramą internetową/proxy Zamawiającego. 9. Tokenizacja (zastępowanie wrażliwego elementu danych, na przykład numer konta bankowego, niewrażliwym substytutem, zwanym tokenem) lub szyfrowanie danych nie może ograniczać funkcjonalności chronionej aplikacji. Jeśli polityka CASB nakazuje, aby dane były tokenizowane lub szyfrowane, funkcjonalność usługi chmurowej nie powinna być ograniczona. 10. Przyjazny interfejs użytkownika (UI). CASB powinno zapewnić prosty UI, który zapewnia autoryzowanym użytkownikom dostęp do kluczowych informacji w oparciu o role. 11. Architektura o wysokiej dostępności. Platforma CASB musi być stale dostępna z poziomem Recovery Time Objective (RTO) mniejszym niż 1h w przypadku awarii komponentów lub przestoju centrum danych – akceptowalny poziom SLA dla CASB 99,999%. 12. Elastyczność i skalowalność. Rozwiązanie CASB musi być zdolne do skalowania, aby wspierać zarówno liniowy

		wzrost, jak i nieprzewidziane skoki aktywności. 13. Brak zauważalnego wpływu na wydajność aplikacji. Gdy użytkownicy uzyskują dostęp do chronionej aplikacji poprzez CASB, w trybie proxy, nie mogą zauważyć żadnego wpływu na wydajność. 14. Raportowanie. CASB musi zapewnić raportowanie, które obejmuje m.in. wiarygodność dostawcy usług w chmurze oraz dostęp użytkowników i urządzeń, zdarzenia i alarmowanie. CASB powinno mieć możliwość filtrowania i dostosowywania tych raportów.
	Threat Protection	1. Zapewnienie ścieżki audytu wszystkich działań i czynności związanych z dostępem. CASB musi dostarczyć kompletny dziennik wszystkich działań, które monitorował, wraz z kompletną ścieżką audytu podjętych działań w zakresie egzekwowania polityki (takich jak blokowanie, kwarantanna, lub zwiększone prośby/próby o uwierzytelnienie). 2. Identyfikacja zdarzeń na podstawie analityki zachowań użytkowników (UEBA). CASB musi dostarczyć rozwiązanie UEBA, które zawiera monitorowanie aktywności użytkowników i wykrywanie anomalii w celu włączenia polityki bezpieczeństwa i alertów. 3. Identyfikacja i remediacja dla zagrożony kont. CASB musi posiadać mechanizmy identyfikacji kont, które mogły zostać skompromitowane i zainicjować automatyczne działania w celu remediacji kont, takie jak wygenerowanie zdarzenia, alertu i zablokowanie dostępu do konkretnego konta. Na przykład, konto użytkownika w chronionej aplikacji jest wykorzystywane w PL, a następnie w tym samym czasie lub w małym oknie czasowym, np. 2 godziny jest uzyskiwany dostęp do tej samej chronionej aplikacji z fizycznie niemożliwej do uzyskania lokalizacji w tak krótkim czasie, np. w Chinach. 4. Zapewnienie przetwarzania zdarzeń (anomalii) i alertów. Gdy zdarzenie/anomalia od polityki zostanie wykryta przez CASB, dane o tym wyjątku/anomalii muszą być dostarczone wybranej grupie analityków bezpieczeństwa do zbadania za pomocą zautomatyzowanego, definiowalnego przez administratora mechanizmu.

ul. Chmielna 69, 00-801 Warszawa
tel. +48 22 39 07 401
gov.pl/NCBR

		5. Zapewnienie automatyzacji przepływu pracy. CASB musi zapewnić możliwość włączenia przepływów pracy, takich jak eskalacja w określonym przedziale czasu, gdy określone zdarzenia/anomalie lub alerty są generowane z powodu naruszenia polityki. 6. Integracja z systemem Security Information and Event Management (SIEM). Zdarzenia, alerty i inne aktywności z CASB muszą mieć możliwość integracji z istniejącą u Zamawiającego infrastrukturą SIEM, aby zapewnić jednolity widok dla zespołu bezpieczeństwa. 7. Zapewnienie dostępu do danych historycznych. CASB musi być w stanie dostarczyć dane zespołom Incident Response (IR) i forensic po wystąpieniu podejrzanej aktywności. Na przykład, dla podejrzanego użytkownika, jakie działania wykonał on ostatnio i czy wykonał on jakiekolwiek działania administracyjne. 8. Zapewnienie dynamicznej analizy złośliwego oprogramowania. CASB musi być w stanie monitorować dane przechowywane w aplikacjach w chmurze i wykrywać, czy w plikach znajduje się złośliwe oprogramowanie. Ta zdolność powinna być dostępna zarówno w czasie rzeczywistym dla konfiguracji proxy, jak i poprzez "crawling" dla integracji opartych na API.
	Zarządzanie ryzykiem dostawcy usług w chmurze	1. Zapewnienie oceny ryzyka usług w chmurze. CASB musi być w stanie zapewnić ocenę wiarygodności lub ocenę ryzyka dla wykrytych usług w chmurze, aby pomóc w określeniu, które usługi wymagają natychmiastowego działania, np. zablokowania lub silnej kontroli dostępu. 2. Analiza i śledzenie podatności i exploitów dostawcy CASB. Producent CASB musi prowadzić bieżące śledzenie aktualnych podatności i wskazywać status dostawców usług w chmurze w interfejsie użytkownika CASB.
	Kontrola dostępu	1. Zapewnienie kontroli dostępu do skategoryzowanych usług w chmurze. CASB musi kategoryzować i nadawać priorytety usługom w chmurze i stosować polityki kontroli dostępu w oparciu o poziom zaufania. Na przykład "zaufane" usługi, do których dostęp może mieć każdy; "niezaufane" usługi, które są zablokowane przez cały czas; oraz "nie w pełni zaufane" usługi, które muszą być dokładnie monitorowane i kontrolowane.

		2. Integracja z usługami zarządzania tożsamością i dostępem (IAM). CASB musi integrować się z istniejącą infrastrukturą bezpieczeństwa firmy, która obsługuje tożsamość użytkowników - zarówno wewnętrznie, jak i w chmurze. Obejmuje to Single Sign-On (SSO) i federacyjne zarządzanie tożsamością. 3. Wsparcie dla standardowych dla branży protokołów federacyjnych. CASB musi być konfigurowalny do pracy z branżowymi standardowymi federacyjnymi technologiami i protokołami uwierzytelniania, autoryzacji i dostarczania użytkowników, w tym (ale nie tylko) SAML, ADFS, OAuth i SCIM. 4. Integracja z narzędziami korporacyjnymi w celu zapewnienia wielopoziomowego uwierzytelniania na podstawie polityki. CASB musi zapewnić zdolność do wymagania wielopoziomowego uwierzytelniania (2FA) w oparciu o politykę, w połączeniu z rozwiązaniami korporacyjnymi, które mogą być na miejscu (onprem) lub w chmurze. Jako przykład, konkretny użytkownik uruchamia politykę opartą na serii zdarzeń, jednym z potencjalnych działań może być poproszenie użytkownika o dostarczenie innej warstwy uwierzytelniania, takich jak OTP lub identyfikator oparty na SMS. 5. Zapewnienie kontekstu tożsamości i zastosowanie do polityk kontroli dostępu. CASB musi dostarczać dane kontekstowe, w tym między innymi takie rzeczy jak użytkownik, urządzenie, lokalizacja, usługa, sieć, pora dnia i rodzaj danych. CASB musi następnie być w stanie wykorzystać te punkty danych w politykach kontroli dostępu do chronionych usług w chmurze. 6. Zapewnienie polityki kontroli dostępu na podstawie aktywności użytkownika. CASB musi zapewnić kontrolę dostępu w oparciu o konkretne działania podejmowane przez użytkownika. Przykładem tego może być sytuacja, w której organizacja zdecydowała, że Google Drive jest "niezaufane", ale zdecydowała, że Microsoft OneDrive jest "zaufane" - jednakże partner biznesowy dzieli się dokumentem z pracownikiem używając Google Drive. W tym przypadku nadal chcemy, aby pracownik mógł uzyskać dokument, ale nie chcemy, aby cokolwiek tam

		przesyłał. 7. Obsługa zarówno osobistych jak i firmowych poświadczeń z odpowiednimi politykami. CASB musi być w stanie skonfigurować i zastosować polityki odpowiednio w zależności od tego, czy dany użytkownik używa poświadczeń firmowych czy osobistych na zarządzanym urządzeniu. Przykładem może być sytuacja, w której firma ma "zaufanego" firmowego Dropboxa, ale nie chce, aby jakiekolwiek dane korporacyjne trafiały do osobistego Dropboxa pracownika. 8. Obsługa współdzielonych poświadczeń z odpowiednimi politykami. CASB musi być w stanie skonfigurować i zastosować odpowiednie polityki dla użytkowników uzyskujących dostęp do współdzielonego konta firmowego podczas korzystania z firmowych poświadczeń. Przykładem tego może być zezwolenie na korzystanie z np. Twittera tj. firmowego współdzielonego konta, podczas gdy inne poświadczenia będą ignorowane, lub zapewniane inne polityki, dla użytku osobistego. 9. Obsługa polityk kontroli dostępu specyficznych dla danego kraju. CASB musi być konfigurowalny pod kątem wymagań kontroli dostępu specyficznych dla danego kraju, takich jak na przykład umożliwienie dostępu do Office365 z UE, ale zablokowanie dostępu z innych krajów np. Chiny.
	Data Loss Prevention (DLP)	1. Zapewnienie zaawansowanego DLP opartego na politykach. CASB musi być w stanie zapewnić podejście do DLP oparte na politykach. Funkcjonalność DLP powinna być na tyle dojrzała, aby umożliwić CASB inspekcję i ochronę krytycznych danych w dokumentach i metadanych. CASB DLP powinno również zapewniać funkcje takie jak fingerprinting, dokładne dopasowanie, wsparcie międzynarodowe, słowniki oraz mechanizmy walidacji takie jak testy Luhna dla numerów kart kredytowych. 2. Zapewnienie cloud DLP poprzez API. CASB musi być w stanie zapewnić monitorowanie danych w czasie zbliżonym do rzeczywistego, wykorzystując API dostarczone przez aplikację w chmurze i zastosować

		alarmowanie, szyfrowanie lub wstrzymanie dostępu do elementów, które spełniają kryteria naruszenia polityki. 3. Zapewnienie DLP poprzez proxy. CASB musi być w stanie zapewnić monitorowanie danych w czasie rzeczywistym, poprzez połączenie proxy pomiędzy użytkownikiem, a aplikacją w chmurze i zastosować miedzy innymi takie akcje jak blokowanie, ostrzeganie, szyfrowanie lub zatrzymanie dostępu do elementów, które spełniają kryteria naruszenia polityk dlp. 4. Zapewnienie rozpoznawania wzorów danych. CASB musi być w stanie rozpoznać dane podlegające regulacji, takie jak dane osobowe, chronione informacje zdrowotne, numery PESEL, numery klientów, klasyfikacje danych itp. 5. Zapewnienie inspekcji HTTPS / bezpiecznego transportu. CASB musi mieć możliwość inspekcji ruchu przesyłanego przez HTTPS w celu zastosowania polityki do danych w tranzycie podczas działania w trybie Proxy. 6. Zapewnienie szyfrowania/tokenizacji danych w ruchu/ w spoczynku. CASB musi obsługiwać elastyczne szyfrowanie i/lub tokenizację wrażliwych danych podczas interakcji z aplikacjami chmurowymi. 7. Odczyt / zastosowanie znaczników klasyfikacji danych. CASB musi być w stanie wykorzystywać znaczniki identyfikacyjne z aplikacji natywnych lub aplikacji stron trzecich i włączyć je do polityk dlp. CASB musi w wspierać wykorzystywany prze Zamawiającego mechanizm klasyfikacji informacji. 8. Włączenie automatycznych działań po naruszeniu polityki. W przypadku naruszenia zasad ochrony danych CASB musi być w stanie wykonać odpowiednie skonfigurowane działanie, które mogą obejmować szyfrowanie, alarmy, logowanie, blokowanie działania, kwarantannę danych do czasu uzyskania akceptacji na realizowaną czynność. 9. Zapewnienie elastycznego zarządzania kluczami i przechowywania kluczy. CASB musi wspierać elastyczne rozwiązania w zakresie zarządzania kluczami szyfrowania, w tym klucze zarządzane przez klienta z wykorzystaniem rozwiązania on-premise lub podejścia opartego na sprzętowym module bezpieczeństwa

		(HSM) w chmurze. 10. Zapewnienie wsparcia dla plików, które są zablokowane lub zaszyfrowane. CASB musi zapewnić możliwości DLP, gdy pliki, które są przesyłane do chmury są chronione hasłem, mają DRM lub są w inny sposób zablokowane/zaszyfrowane. 11. Zapewnienie kontroli dostępu na niezarządzanych urządzeniach. CASB musi zapewnić mechanizmy integracji z niezarządzanymi urządzeniami BYOD i zapewnić DLP sterowane polityką w zależności od potrzeb, nawet gdy nie ma oprogramowania MDM.
	Widoczność	1. Identyfikacja aplikacji chmurowych w użyciu. CASB musi być w stanie wykryć i wyświetlić "Shadow IT" poprzez wykrywanie pełnego zakresu znanych aplikacji chmurowych w użyciu, niezależnie od tego, czy CASB jest skonfigurowany w trybie wykrywania opartym na logach, czy w trybie aktywnego proxy. 2. Odkrywanie aplikacji w chmurze opartych na Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) i Infrastructure-as-a-Service (IaaS). CASB musi być w stanie wykryć i wyświetlić usługi IaaS i PaaS w użyciu, niezależnie od tego, czy CASB jest skonfigurowany w trybie wykrywania opartym na logu lub aktywnym trybie proxy. 3. Identyfikacja poszczególnych użytkowników aplikacji chmurowych. CASB musi być w stanie wykryć i wyświetlić konkretnych użytkowników aplikacji chmurowych najlepiej po nazwie lub alternatywnie po ID użytkownika. 4. Identyfikacja urządzenia dla użytkowników aplikacji chmurowych. CASB musi być w stanie wykryć i wyświetlić konkretne urządzenie i przeglądarkę (jeśli dotyczy) dla użytkowników aplikacji chmurowych. 5. Identyfikacja typu urządzenia. CASB musi być w stanie wykryć i wyświetlić status urządzenia oraz urządzenia, które są używane, takie jak laptopy lub inne urządzenia. 6. Identyfikacja danych lokalizacyjnych dla użytkowników usług w chmurze. CASB musi być w stanie wykryć i wyświetlić informacje o lokalizacji, geograficznej i IP, z którego odbywa się dostęp. 7. Identyfikacja rodzajów danych przechowywanych w

		usługach w chmurze. CASB musi być w stanie zidentyfikować, jakie elementy danych (pliki, pola) są przechowywane w zidentyfikowanych usługach w chmurze lub wykorzystywane za ich pomocą, a także wskazać elementy o znacznym ryzyku dotyczącym danych.
2	Gwarancja, serwis i wsparcie techniczne producenta	1. Długość gwarancji i wsparcia producenta zgodnie z ofertą, lecz nie krócej niż 24 miesiące miesięcy, 2. Gwarancja i serwis realizowany zdalnie, z czasem reakcji w zależności od poziomu krytyczności awarii/błędy od 1 do 48 godzin od przyjęcia zgłoszenia (szczegóły niżej), możliwość zgłaszania awarii poprzez dedykowany i zabezpieczony kanał komunikacji elektronicznej. 3. Producent musi umożliwiać skuteczne zgłaszanie awarii w trybie 24x7x365 poprzez system zgłoszeniowy producenta. 4. Gwarancja i serwis realizowany w trybie 8x5 4h-48h Remote Response Time (dla niekrytycznego poziomu błędu/awarii) oraz 24x7x365 1h Remote Response Time (w przypadku krytycznego poziomu błędu/awarii). 5. Zakres wsparcia technicznego a. Dostęp do pomocy technicznej; b. Dostęp do poprawek, nowych wersji oprogramowania; c. Dostęp do dokumentacji technicznej; d. Dostęp do konta wsparcia, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta. 6. Szczegółowe warunki wsparcia technicznego dla Oprogramowania, o którym mowa powyżej regulować powinny umowy licencyjne lub inne stosowne umowy lub warunki wydane lub zaakceptowane przez producenta Oprogramowania, przy czym umowy takie, ani warunki nie mogą ograniczać wskazanych powyżej wymagań, ani stać z nimi w sprzeczności
3	Dokumentacja	1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
4	Licencja	1. Rządowa (jeśli jest to możliwe, w przeciwnym wypadku komercyjna) 2. Na okres 24 miesięcy

6	Wymagania w zakresie instalacji i konfiguracji	1. Brak – instalacja, konfiguracja realizowana przez Zamawiającego