Załącznik nr 2 do SWZ

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**Dostarczenie i wdrożenie:**

**- systemu antywirusowego i systemu EDR dla stacji roboczych i serwerów w szczególności systemu HIS.**

**-systemu do kopii bezpieczeństwa w systemie chmurowym.**

**- poczty internetowej.**

**Wykonawca dostarczy system klasy enterprise zapewniający ochronę stacji roboczych i serwerów w architekturze client-serwer umożlwiający również monitorowanie aplikacji HIS wykorzystywanej w placówce pod kątem bezpieczeństwa bibliotek programistycznych aplikacji HIS oraz bezpieczeństwa komunikacji HIS z systemami zewnętrznymi z wykorzystaniem interfejsów API. System powinien zostać dostarczony jako licencje lub subskrypcje, w przypadku modelu subskrypcyjnego konieczne jest dostarczenie 36 miesięcznej subskrypcji. W przypadku licencji, jak i subskrypcji system powinien być objęty wsparciem producenta na warunkach producenta na okres min. 36 miesięcy.**

**System powinien spełniać następujące wymagania funkcjonalne:**

1. **Komponent Ochrony Stacji Roboczych:**
2. **Administracja zdalna**

1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.

2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.

3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.

4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.

5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.

6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.

7. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.

8. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).

9. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.

10. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.

11. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

12. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.

13. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.

14. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.

15. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

1. **Ochrona stacji roboczych**

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).

2. Rozwiązanie musi wspierać architekturę ARM64.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.

5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.

9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.

10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.

12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.

15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

* + tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
	+ tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
	+ tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
	+ tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
	+ tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

21. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego MS Outlook.

22. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

* + tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
	+ tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
	+ tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
	+ tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

23. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.

24. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

25. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.

27. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.

28. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

29. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

1. **Ochrona serwera**

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.

2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.

8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).

11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.

12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.

15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.

20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

1. **Szyfrowanie**

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.

2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).

3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.

4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.

2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.

3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

4. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.

5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:

1. nazwę aplikacji,
2. nazwę pakietu,
3. kategorię sklepu Google Play,
4. uprawnienia aplikacji,
5. pochodzenie aplikacji z nieznanego źródła
6. **Komponent monitorowania podatności**
7. **Wymagania ogólne**
	1. Monitorowanie aplikacji ma odbywać się w sposób ciągły, z wykorzystaniem oprogramowania monitorującego. Część centralna oprogramowania może być udostępniona w modelu SaaS.
	2. Rozwiązanie oparte o model SaaS musi zapewniać poziom bezpieczeństwa potwierdzony min. Certyfikatem SOC-2 lub równoważnym. Rozwiązanie powinno być zgodne z zasadami dyrektywy GDPR oraz zapewniać, że dane w SaaS będą przechowywane oraz przetwarzane na terenie Unii Europejskiej. Komunikacja pomiędzy komponentami rozwiązania w SaaS a komponentami w infrastrukturze Zamawiającego musi być szyfrowana z wykorzystaniem min. AES-256 lub równoważnym, komunikacja może się odbywać jedynie jednokierunkowo – od strony komponentów zlokalizowanych w infrastrukturze Zamawiającego do SaaS.
	3. Oprogramowanie musi być dostępne w postaci interfejsu graficznego z poziomu przeglądarki internetowej.
	4. Dostęp do oprogramowania musi był zabezpieczony hasłem. Autentykacja i autoryzacja w oprogramowaniu ma umożliwiać kontrolę dostępu opartą na rolach (RBAC)
	5. Oprogramowanie wykorzystywane dla świadczenia usługi musi umożliwiać́ integrację bazy użytkowników z LDAP.
	6. Dostęp do oprogramowania musi zapewniać zabezpieczenie dostępu z poziomu operatora i użytkownika oprogramowania za pomocą̨ protokołu HTTPS.
	7. Elementy oferowanego rozwiązania muszą w zakresie komunikacji (wewnętrznej i zewnętrznej) umożliwiać wykorzystywanie protokołów bezpieczeństwa, przynajmniej SSL.
8. **Dostarczony system zapewni:**
	1. Ciągłe monitorowanie istniejących, znanych podatności, istniejących lub takich, które pojawią się w czasie świadczenia usługi i zostaną sklasyfikowane za pomocą sygnatur podatności CVE oraz CVSS.
	2. Zamawiający uzyska ciągły (24/7h) dostęp do bazy informacji na temat podatności w systemach Systemu w taki sposób aby mógł uzyskać informację o:
9. Stosowanych w Systemie bibliotekach programistycznych.
10. Powiązaniu bibliotek w konkretnymi procesami aplikacyjnymi i wykonywanymi metodami.
11. Podatnościach tychże bibliotek lub ich braku.
12. Poziomie krytyczności wykrytych podatności ze wskazaniem, które z podatności mają charakter krytyczny, wysoki, średni oraz niski.
13. Wadze punktowej od 1-100, określającej poziom zagrożenia związanego z wykrytą podatnością.
14. Czy dla wykrytych podatności istnieją metody ich wykorzystania.
15. Czy dana podatność jest aktywnie wykorzystywana.
16. Listę przeprowadzonych prób wykorzystywania podatności wraz określeniem czasu incydentu.
17. Krótki opis wykrytej podatności wraz z sugerowanym sposobem jej usunięcia jeśli taki istnieje.
18. Poziomie bezpieczeństwa zapytań API do systemów zewnętrznych dla Systemu.
	1. Wykonawca zapewni ciągłą aktualizację informacji określonych w pkt 2.
	2. Wykonawca zapewni automatyczne alertowanie za pomocą zapytania HTTP w przypadku wykrycia nowych podatności.
	3. Oprogramowanie musi umożliwić zdefiniowane możliwej reakcji na próbę wykorzystania podatności np. zignorowanie, śledzenie lub jej automatyczne zablokowanie.
	4. Dostarczone oprogramowanie musi być oparte o dane min. jednej organizacji Thread Intelligence, dostępne w sposób ciągły bez konieczności instalowania żadnych komponentów sprzętowych w infrastrukturze Zamawiającego.
19. **Monitorowanie musi zapewniać:**
	1. Możliwość uruchomienia monitoringu dla aplikacji pracujących przynajmniej na następujących systemach operacyjnych:
		1. AIX
		2. Linux:
			* CentOS
			* Debian
			* Fedora
			* openSUSE Leap
			* Red Hat Enterprise Linux
			* SUSE Linux Enterprise
			* Ubuntu
		3. Windows:
			* 2012
			* 2012 R2
			* 2016
			* 2019
			* 2022
	2. Oprogramowanie powinno zapewniać możliwość monitorowania wielowarstwowych aplikacji wykonanych w następujących technologiach:
		1. Java
		2. .Net
	3. Na podstawie wykrytych przepływów, w sposób automatyczny pozwala odwzorować w formie graficznej monitorowany system obrazując powiązania i zależności monitorowanych komponentów i procesów oraz ich wzajemną komunikację, w szczególności uwzględniając takie warstwy jak serwery aplikacyjne, bazy danych, zewnętrzne serwisy i kolejki. W przypadku wykrycia odstępstwa od normy skutkującej wygenerowaniem alertu, monitorowany komponent, musi zostać oznaczony na wizualizacji w sposób jednoznacznie wskazujący na wystąpienie problemu w danym miejscu.
	4. Wykrywa i monitoruje przebieg wszystkich transakcji przepływających przez aplikację w sposób automatyczny oraz oferuje możliwość ręcznego dostosowania sposobów wykrywania i monitoringu transakcji. Oprogramowanie musi wspierać definiowanie własnych transakcji biznesowych na podstawie spersonalizowanych reguł dopasowania, opartych o:
		1. URL
		2. wartość parametru z nagłówka HTTP,
		3. wartość parametru z zapytania GET lub POST,
		4. wykonanie konkretnej metody w kodzie Java lub .NET,
		5. wywołanie konkretnej usługi WebService.
	5. Automatycznie wykrywa rodzaje komunikacji pomiędzy wykrytymi komponentami monitorowanych aplikacji, a w tym wspiera śledzenie transakcji wykorzystujących co najmniej następujące technologie synchroniczne i asynchroniczne:
		1. HTTP
		2. REST
		3. SOAP/XML
		4. JMS
	6. Oferuje możliwość uzyskania następujących informacji o wybranych transakcjach:
		1. drzewo wywołania kodu oprogramowania w ramach transakcji uwzględniając nazwy wywoływanych metod, zarówno dla wątków wywoływanych synchronicznie jak i asynchronicznie wraz z czasem wykonania pojedynczych metod,
		2. czasach odpowiedzi serwera do aplikacji klienckiej jak i całkowitym czasie wykonania transakcji po stronie serwera (wątków synchronicznych oraz asynchronicznych),
		3. zapytaniach SQL wykonanych w ramach transakcji z możliwością uzyskania informacji o użytych w nich zmiennych lub celowego ich maskowania,
		4. wartościach parametrów wywołania wskazanych metod,
		5. wartościach zwracanych przez wskazane metody.
	7. Oprogramowanie musi umożliwiać korelację transakcji realizowanych przez monitorowane komponenty z odpowiadającymi im danymi infrastrukturalnymi, bazodanowymi i sesją użytkownika końcowego.
	8. Umożliwia automatyczne wytwarzanie linii bazowych dla wszystkich metryk kolekcjonowanych przez dostarczone oprogramowanie, które są wyliczane z uwzględnieniem sezonowości w charakterystyce zapytań przepływających przez aplikację, z uwzględnieniem dni, tygodni i miesięcy (z rozdzielczością godzinną). Zamawiający musi mieć możliwość definiowania własnych linii bazowych, budowanych na podstawie kroczącego okresu czasu i na podstawie danych pobieranych w odstępach dziennych, tygodniowych lub miesięcznych.
	9. Oprogramowanie musi udostępniać reguły powiadamiania w przypadku wykrycia problemów z wydajnością w aplikacji lub innych anomalii w oparciu o automatycznie wygenerowane linie bazowe lub statyczne wartości.
	10. Oferowane oprogramowanie musi automatycznie, na podstawie danych bazowych/wzorcowych wykrywać problemy związane co najmniej z:
		1. wydłużeniem czasów odpowiedzi poszczególnych usług po stronie serwerowej,
		2. zwiększeniem poziomu problemów dla poszczególnych usług po stronie serwerowej,
		3. wydłużeniem czasów odpowiedzi dla poszczególnych akcji wykonywanych przez użytkownika końcowego na aplikacji WWW lub aplikacji mobilnej,
		4. zwiększeniem poziomu problemów dla poszczególnych akcji wykonywanych przez użytkownika końcowego na aplikacji WWW lub aplikacji mobilnej,
		5. przeciążeniem CPU,
		6. nadmiernym wykorzystaniem pamięci,
		7. spadkiem wydajności dysków,
		8. brakiem dostępności aplikacji.
	11. Umożliwia definiowanie, konfigurację i modyfikację reguł, na podstawie których oprogramowanie generuje alerty. Oprogramowanie musi mieć możliwość wygenerowania alertu na podstawie zadanego odchylenia danej metryki od wyżej wspomnianej linii bazowej lub na podstawie statycznego progu. Funkcjonalność ta musi umożliwiać tworzenie złożonych warunków generowania tych alertów przy użyciu wyrażeń logicznych.
	12. Na podstawie wygenerowanego alertu, musi umożliwiać wykonanie automatycznie następujących akcji:
		1. Wysłanie powiadomienia do konkretnych użytkowników za pomocą wiadomości SMS lub e-mail,
		2. Uruchomienie dokładnej diagnostyki dla monitorowanych transakcji biznesowych, dla których został wygenerowany alert,
		3. Automatyczne wykonanie zrzutu wątku dla technologii Java (ang. thread dump),
		4. Wykonać dowolny skrypt na monitorowanym serwerze aplikacyjnym,
		5. Wysłać zapytanie HTTP o dowolnej treści na dowolny URL.
	13. W opcji instalowania części centralnej Oprogramowania w infrastrukturze Zamawiającego, pozwala definiować własne spersonalizowane akcje, które mogą być uruchamiane jako efekt wygenerowania przez Oprogramowanie alertu, które pozwalają na integrację z zewnętrznymi narzędziami używanymi przez Zamawiającego takimi jak systemy do śledzenia problemów i projektów.
	14. Oprogramowanie musi posiadać mechanizm przeciwdziałania generowania fałszywych alertów.
	15. Pozwala zbierać i monitorować najbardziej wpływające na wydajność monitorowanej aplikacji zapytania SQL wykonywane z poziomu monitorowanej aplikacji z możliwością ich powiązania z transakcjami, które dane zapytania wykonują.
	16. Ogranicza swój wpływ na monitorowane platformy i aplikacje m.in poprzez inteligentne zbieranie informacji celem uniknięcia zbędnego zużywania zasobów. Dodatkowo rozwiązanie musi oferować możliwość zbierania zwiększonego zakresu informacji poprzez manualne wyłączanie mechanizmu ograniczania narzutu na zasoby monitorowanego serwera dla wybranych transakcji biznesowych lub serwerów aplikacyjnych, np. w celach diagnostycznych lub testowych.
	17. Posiada możliwość prezentowania na wykresach dowolnych metryk gromadzonych przez oprogramowanie.
	18. Pozwalać na tworzenie dowolnych niestandardowych pulpitów prezentujących gromadzone w ramach usługi dane, z poziomu interfejsu graficznego. Oprogramowanie musi umożliwiać nadawanie użytkownikom uprawnień́ wyświetlania lub edycji poszczególnych pulpitów.
	19. Wykonawca w ramach dostarczonego oprogramowania musi w przypadku wykrycia problemu automatycznie wskazać możliwe przyczyny wystąpienia problemu.
	20. Wykonawca musi gwarantować odpowiedni poziom dostępu do danych definiowany na poziomie nadawania uprawnień do dostarczonego oprogramowania oparty o system ról i grup użytkowników (ang. Role-Based Access Control). Mechanizm konfiguracji uprawnień musi być dostępny w interfejsu graficznego jak i z poziomu interfejsu API dostarczonego oprogramowania, służącego wykonywaniu usługi.
	21. Oprogramowanie musi umożliwiać porównywanie działania aplikacji w różnych przedziałach czasowych na poziomie czasów odpowiedzi, liczby błędów, poziomu ruchu i tym podobnych.
	22. Oprogramowanie musi zbierać informacje o wszystkich błędach i wyjątkach. Musi istnieć możliwość zobaczenia szczegółowych informacji na temat transakcji, w których wystąpił błąd bądź został wygenerowany wyjątek.
	23. Oprogramowanie, poza domyślnym mechanizmem detekcji problemów, musi oferować możliwość konfiguracji tzw. wyjątków – odstępstwa od reguły, pozwalające na odrzucenie błędów technicznych, które nie mają wpływu na biznesowe działanie aplikacji.
	24. Dostarczone oprogramowanie musi zapewniać wyszukiwanie w zgromadzonym przez niego zbiorze danych dotyczących transakcji na podstawie definiowalnych filtrów lub zapytań. Musi istnieć możliwość definiowania wielu filtrów lub zapytań wraz z możliwością ich zapisu celem ciągłego lub wielokrotnego użycia. Administrator lub użytkownik oprogramowania musi mieć również możliwość utworzenia niestandardowych metryk na podstawie wcześniej wspomnianych filtrów lub wyszukiwań. Dla tych niestandardowych metryk, Oprogramowanie również musi automatycznie wygenerować linie bazowe.
	25. Dostarczone oprogramowanie musi pozwalać na użycie operatorów logicznych, wzorców, wyrażeń regularnych (REGEX) w filtrach lub zapytaniach używanych do przeszukiwania danych dotyczących transakcji.
	26. Dostarczone oprogramowanie musi posiadać możliwość tworzenia lub konfigurowania definiowanych przez Administratora lub użytkownika aplikacji dodatkowych niestandardowych wtyczek monitorujących. Dla metryk dostarczanych przez te dodatkowe wtyczki, Oprogramowanie musi automatycznie wygenerować linie bazowe.
	27. Oprogramowanie musi posiadać funkcjonalność logowania wszystkich aktywności użytkowników związanych ze zmianami konfiguracji. Logowanie musi umożliwiać jednoznaczne wskazanie osoby, która wykonała zmianę.
	28. Dostarczone oprogramowanie - musi oferować także udokumentowany interfejs programistyczny (API) służący do konfiguracji Oprogramowania, pobierania danych, a w tym metryk historycznych.
	29. Pozwala analizować wpływ zmian wersji oprogramowania na wydajność procesów, transakcji oraz wartość metryk związanych z obsługą użytkowników aplikacji, celem wskazania czy wprowadzane zmiany prowadzą do pożądanego stanu funkcjonowania aplikacji. Oprogramowanie musi oferować możliwość rejestracji zdarzenia wgrania nowej wersji aplikacji.
	30. Posiada możliwość budowania i wizualizacji niestandardowych, złożonych ścieżek biznesowych wykonywanych przez użytkowników w aplikacji połączonych unikalnym identyfikatorem, celem analizy czasu jaki zajmuje użytkownikom wykonanie poszczególnych kroków.
20. **W zakresie monitorowania użytkownika końcowego, oprogramowanie musi spełniać poniższe wymagania techniczne i posiadać niżej wymienione funkcje:**
	1. Pozwala na monitorowanie sposobu działania aplikacji z perspektywy przeglądarek internetowych użytkowników końcowych w zakresie czasu odpowiedzi aplikacji i występujących błędów.
	2. Przedstawia informacje w jaki sposób użytkownicy końcowi wchodzą w interakcję z aplikacją i w jaki sposób w niej nawigują.
	3. Przedstawia wpływ sieci i czasu wczytywania aplikacji po stronie przeglądarki internetowej na doświadczenia użytkownika końcowego.
	4. Pozwala na zbieranie danych dotyczących używanej przeglądarki, systemu operacyjnego, wykorzystywanego urządzenia i innych parametrów pozwalających na identyfikację jak aplikacja działa dla różnych grup użytkowników.
	5. Oprogramowanie musi umożliwiać powiązanie monitorowane sesji użytkownika końcowego z interakcją z systemem i transakcjami realizowanymi przez system na poziomie sekwencji wywołanych metod i skorelowanych informacji infrastrukturalnych, od rozpoczęcia aktywności (np. dostęp do strony WWW), aż do jej zakończenia (np. odpowiedź bazy danych).
	6. Oprogramowanie musi umożliwiać automatyczne sprawdzanie dostępności i wydajności aplikacji poprzez cykliczne lub jednorazowe wykonywanie skryptu symulującego pracę użytkownika. Administrator lub użytkownik oprogramowania musi mieć możliwość definiowania skryptów symulujących pracę użytkownika z zastosowaniem biblioteki Selenium WebDriver.
	7. Oprogramowanie musi pozwalać na geolokalizację zdarzeń na bazie adresów IP oraz umożliwiać jej wizualizacje na mapie.
	8. Oprogramowanie musi pozwalać na mapowanie danych geolokalizacyjnych dla wewnętrznej adresacji IP poprzez wprowadzenie wymaganych danych przez interfejs web lub plik z danymi geolokacyjnymi.
	9. Pozwala na monitorowanie działanie aplikacji w wersji mobilnej dla systemów Android i iOS.
	10. Umożliwia robienie zrzutów ekranów aplikacji mobilnych w systemach Android i iOS.
21. **W zakresie monitorowania baz danych, oprogramowanie musi spełniać poniższe wymagania techniczne i posiadać niżej wymienione funkcje:**
	1. Umożliwia monitorowanie następujących baz danych:
		1. Apache Cassandra
		2. Datastax Enterprise (DSE) Cassandra
		3. IBM DB2 (instalowanych na OS Linux, Ubuntu oraz Windows)
		4. MongoDB
		5. MySQL
		6. Microsoft SQL Server
		7. Oracle
		8. PostgreSQL
	2. Umożliwia monitorowanie baz danych będących częścią monitorowanego środowiska, celem wykrycia źródeł problemów wydajnościowych, zarówno z punktu widzenia wykonywania zapytań i procedur zainicjowanych przez monitorowane aplikacje jak i przez inne podmioty nieobjęte monitoringiem.
	3. Monitoruje bazy danych w sposób nie wymagający instalacji agenta na hoście bazy danych.
	4. Zapewnia informacje dotyczące zużycia zasobów serwera bazy danych takich jak CPU, Pamięć, I/O dysku i I/O sieci.
	5. Zapewnia ogólne informacje dotyczące ilości zapytań wykonywanych w bazie w zadanym okresie czasu wraz z czasem spędzonym na ich wykonywaniu.
	6. Zapewnia informacje dotyczące stanów oczekiwania (ang. Wait States) wraz z dystrybucją czasu spędzonego w każdym ze stanów oczekiwania.
	7. Zapewnia informacje na temat zapytań i procedur, które zajmują najwięcej czasu w bazie danych przedstawiając ich składnie, ilość wykonań lub ilość wykonywujących je sesji oraz czas spędzony na wykonywaniu, jednocześnie pozwalając na grupowanie zapytań i procedur o tej samej lub zbliżonej składni.
	8. Zapewnia informacje o nazwach hostów i adresach IP klientów korzystających z baz danych.
	9. Zapewnia informacje o identyfikatorach sesji korzystających z bazy danych wraz z informacją o czasie spędzonym w bazie danych.
	10. Pozwala na uzyskanie informacji dotyczących blokujących się wzajemnie sesji celem zbadania powodów występowania deadlock’ów.
	11. Pozwala na generację i analizę planów zapytań SQL do bazy danych.
	12. Umożliwia definiowanie niestandardowych metryk tworzonych na podstawie zapytań bazodanowych definiowanych przez Administratora lub użytkownika oprogramowania. Dla tych niestandardowych metryk, Oprogramowanie również musi automatycznie wygenerować linie bazowe.
22. **W zakresie gromadzenia, monitorowania i analizy logów, oprogramowanie musi spełniać poniższe wymagania i posiadać niżej wymienione funkcje:**
	1. Musi umożliwiać dostęp do logów aplikacyjnych i systemowych, przeszukiwanie ich i przeglądanie bez konieczności logowania na serwer monitorowany.
	2. Musi zapewniać zbieranie danych wyodrębnianych z plików logów umieszczonych w wyszczególnionym katalogu.
	3. Musi zapewniać́ rozpoznanie formatów czasu i daty w przetwarzanych danych z logów i normalizowanie ich do jednego wspólnego formatu.
	4. Musi zapewniać użytkownikowi posiadającemu uprawnienia samodzielne konfigurowanie reguł odczytu logów w celu umożliwienia analizy zebranych w nich informacji.
23. **Wykonawca zapewni usługę analityczną** w postaci dedykowanego zespołu inżynierskiego w ilości 5 dni, który będzie świadczył na rzecz Zamawiającego Czynności Konsultacyjne w oparciu o Oprogramowanie wykorzystywane do świadczenia usługi monitoringu. Czynności Konsultacyjne powinny w szczególności obejmować:
	1. Wsparcie w procesach: instalacji, konfiguracji, rekonfiguracji agentów systemów operacyjnych, baz danych i aplikacji objętych monitoringiem,
	2. Wsparcie w konfiguracji Oprogramowania zgodnie z potrzebami Zamawiającego (w tym konfiguracja dashboard’ów, alertów),
	3. Transfer wiedzy eksperckiej w zakresie sposobów i możliwości korzystania z Oprogramowania do monitoringu,
	4. Wsparcie w analizie i późniejszej interpretacji danych zebranych przez Oprogramowanie do monitoringu oraz ewentualną asystę w rozwiązywaniu problemów zidentyfikowanych przy użyciu Oprogramowania do monitoringu,
	5. Kompleksowe doradztwo w zakresie najlepszych praktyk dotyczących wykorzystania Oprogramowania.

**Załącznik nr 1. Opis infrastruktury**

1. Na infrastrukturę obsługującą System składają się następujące maszyny wirtualne:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Aplikacja** | **System operacyjny** | **Rodzaj serwera** | **vCPU** | **RAM** | **Technologie** |
| *HIS* | *Oracle Linux Server 7.4* | *Aplikacyjny AMMS Jboss* | *4* | 8 GB | JBOSS |
| DB | *Oracle Linux Server 7.5* | *DB* | *8* | *52 GB* | *Oracle* |
| *P1* | *Oracle Linux Server 7.4* | *Aplikacja Apache* | *4* | *8* | *Apache* |
| EDM | *Oracle Linux Server 7.4* | *Docker* | *2* | *8* | *Docker* |
| Interfejs integrujący | *Oracle Linux Server 7.4* | *Aplikacja Apache* | *4* | *8* | *Apache* |
| PDF Generator | *Windows Server 2016* | *Aplikacja Apache* | *4* | *8* | *Apache* |
| PHIL7 | *Windows Server 2016* | *Aplikacja Apache* | *4* | *10* | *delphi* |
| Zdarzenia Medyczne | *Oracle Linux Server 7.5* | *Aplikacja Apache* | *4* | *8* | *Apache* |

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa | Liczba |
|  | System kopii zapasowej | 1 komplet |

## OPROGRAMOWANIE STANDARDOWE

### Wymagania ogólne

1. Wykonawca jest odpowiedzialny za zaprojektowanie, dostawy licencji i wdrożenie Oprogramowania standardowego ściśle dostosowanego jakościowo i ilościowo do wymagań.
2. Oprogramowanie standardowe dostarczane przez Wykonawcę będzie zaprojektowane, dostarczone, skonfigurowane i wdrożone „pod klucz”.
3. Wykonawca przygotuje dokumentację użytkownika i administratora wdrażanego Oprogramowania.
4. System powinien zostać dostarczony jako licencje lub subskrypcje, w przypadku modelu subskrypcyjnego konieczne jest dostarczenie 36 miesięcznej subskrypcji. W przypadku licencji, jak i subskrypcji system powinien być objęty wsparciem producenta na warunkach producenta na okres min. 36 miesięcy.

### System kopii zapasowej

1. Zamawiający oczekuje dostarczenia jednego, kompletnego systemu backupu spełniającego wszystkie poniższe wymagania. Nie dopuszcza się dostarczenia dwóch odrębnych, zintegrowanych rozwiązań.
2. Dostarczany system kopii zapasowej musi spełniać, co najmniej wymagania przedstawione w tabeli 1 poniżej.
3. Zamawiający wymaga by dostarczone licencje umożliwiały wykonywanie kopii zapasowych, co najmniej:
* 12 maszyn wirtualnych
1. Dostarczany system musi zapewniać możliwość automatycznego wykonywania wyniesionej kopii zapasowej danych, co oznacza przesyłanie i składowanie kopii poza siedzibą Zamawiającego w okresie nie krótszym niż 3 lata od daty podpisania Umowy.
2. W celu realizacji automatycznego wykonywania wyniesionej kopii zapasowej danych, Zamawiający wymaga udostępnienia:
	1. Infrastruktury udostepniającej przestrzeń dyskową na składowanie kopii zapasowych w Centrum Przetwarzania danych spełniającym, co najmniej następujące wymagania:
3. Centrum Przetwarzania Danych musi posiadać aktywne elementy infrastruktury IT zapewniające pracę w modelu n+1;
4. Centrum Przetwarzania Danych musi posiadać redundantne wewnętrzne linie dystrybucji energii elektrycznej obsługujące macierze dyskowe;
5. Centrum Przetwarzania Danych musi posiadać redundantne wewnętrzne linie chłodu równolegle obsługujące macierze dyskowe;
6. Centrum Przetwarzania Danych musi posiadać możliwość, odłączania każdego elementu linii dystrybucji energii elektrycznej i chłodu w celu poddania czynnością serwisowy, tak aby nie zakłócić normalnej pracy urządzeń dwuzasilaczowych;
7. Centrum Przetwarzania Danych musi posiadać wdrożoną strefową kontrolę dostępu w oparciu o karty zbliżeniowe lub rozwiązanie równoważne;
8. Centrum Przetwarzania Danych musi posiadać całodobową ochronę fizyczną z rejestracją kamer monitoringu wizyjnego na zewnątrz i wewnątrz budynku;
9. Centrum Przetwarzania Danych musi być zlokalizowane na terenie Polski;
10. Centrum Przetwarzania Danych musi posiadać niezależne strefy pożarowe oraz system wczesnej detekcji dymu i ognia, a pomieszczenie ze sprzętem IT muszą być wyposażone w zautomatyzowaną aparaturę gaśniczą;
11. Centrum Przetwarzania Danych musi mieć zapewnione zasilanie z dwóch niezależnych linii energetycznych oraz rezerwowe zasilanie realizowane przy pomocy UPS oraz agregatu prądotwórczego;
12. Centrum Przetwarzania Danych musi posiadać UPS’y pracujące w nadmiarowej konfiguracji (co najmniej N+1), zapewniając nieprzerwane zasilanie macierzy dyskowej;
13. Centrum Przetwarzania Danych musi pozwalać, aby dystrybucja energii elektrycznej do macierzy dyskowej odbywała się z wykorzystaniem minimum dwóch niezależnych torów zasilania, z minimum jednym torem gwarantowanym (podtrzymanie zasilania z wykorzystaniem UPS i agregatu prądotwórczego);
14. Centrum Przetwarzania Danych musi posiadać Certyfikat Ochrony Elektromagnetycznej wydany przez Agencję Bezpieczeństwa Wewnętrznego;
15. Centrum Przetwarzania Danych musi spełniać standardy normy EN 50600-1:2019
(dostępność: klasa dostępności 3 lub 4, bezpieczeństwo fizyczne: klasa ochrony 3 lub 4, efektywność energetyczna: poziom szczegółowości 3 lub 4);
	1. Przestrzeni dyskowej na składowanie kopii zapasowej o wielkości 12 TB z możliwością zwiększenia do, co najmniej 100 TB (zwiększenie pojemności powyżej 12 TB nie jest elementem oferty i nie podlega wycenie), w oparciu o wysokodostępną macierz dyskową spełniającą poniższe wymagania:
16. Macierz musi posiadać wbudowaną funkcjonalność sprzętowej deduplikacji;
17. Macierz musi pozwalać na tworzenia kopii zapasowych z wykorzystaniem transmisji wielostrumieniowej;
18. Macierz musi posiadać redundancję wszystkich komponentów – brak pojedynczego punktu awarii. W przypadku awarii kontrolera, automatyczne przełączanie wystawianych zasobów na inny kontroler, którego wydajność jest nie mniejsza niż tego, który uległ awarii.
19. Macierz musi posiadać możliwość rozbudowy w trakcie jej pracy (online);
20. Rozłożenie dysków w macierzy musi zapewniać redundancję pozwalającą na nieprzerwaną pracę i dostęp do wszystkich danych w sytuacji awarii pojedynczego komponentu sprzętowego typu: dysk, półka dyskowa, kontroler, zasilacz;
21. Macierz musi posiadać możliwość aktualizacji firmware trybie online, bez zauważalnego zanikania ścieżek dostępu do zasobów dyskowych macierzy;
	1. Łącza internetowe symetryczne o przepustowości nie mniejszej niż 1 Gb/s do infrastruktury, na której składowane będą wyniesione kopie zapasowe. Wykonawca nie zapewnia łącza po stronie Zamawiającego;
	2. Zamawiający wymaga, aby Wykonawca w zakresie świadczonych usług chmurowych posiadał wdrożone i funkcjonujące normy lub ich odpowiedniki w polskim lub europejskim układzie normalizacyjnym:
22. PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji,
23. PN-EN ISO 22301 dotyczące zarządzania ciągłością działania,
24. ISO/IEC 27017 dotyczące bezpieczeństwa informacji w chmurze obliczeniowej,
25. ISO/IEC 27018 dotyczące dobrych praktyk zabezpieczania danych osobowych w chmurze obliczeniowej
26. Komunikacja pomiędzy Zamawiającym, a miejscem składowania danych wyniesionych musi odbywać się z wykorzystaniem bezpiecznego połączenia (co najmniej SSL lub IPSec).
27. Zamawiający wymaga, aby system przechowywania wyniesionych kopii zapasowych po stronie Wykonawcy nie umożliwiał przesłania niezaszyfrowanej kopii zapasowej do wyniesionego miejsca składania danych.
28. Zamawiający może zażądać wskazania dokładnej lokalizacji fizycznej urządzeń przetwarzania i składowania danych (z dokładnością do adresu i szafy w Centrum Danych).
29. Awaryjne odtwarzanie danych z wyniesionego miejsca składowania danych musi odbywać się automatycznie za pomocą lokalnego interfejsu systemu kopii zapasowych Zamawiającego, bez udziału pracowników Wykonawcy.
30. Wykonawca zapewni panel usługi systemu kopii wyniesionych, który posiada co najmniej poniższe funkcjonalności:
	1. Zdalne monitorowanie i zarządzanie kopiami zapasowymi za pomocą jednego internetowego interfejsu użytkownika.
31. Zabezpieczenie dostępu do Panelu Zarządzania z wykorzystaniem protokołu SSL oraz dwuskładnikowego uwierzytelniania MFA (użytkownik, hasło i token).
32. Prezentacja stanu realizowanych oraz historycznych zadań backupu oraz możliwość eksportowania tych danych do pliku tekstowego.
33. Możliwość uruchamiania, zatrzymywania, powtarzania, włączania i wyłączania zadań backupu oraz pobierania rejestru zdarzeń.
34. Obsługa alarmów dotyczących zadań backupowych oraz stanu systemu oraz eksportowania ich do pliku tekstowego.
	1. Raportowanie i rozliczenia zapewniające pełny wgląd w czasie rzeczywistym w zasoby zaangażowane do przechowywania kopii zapasowych.
35. Możliwość przeglądania raportów.
36. Sprawdzanie poziomu wykorzystania przydzielonej bezpiecznej przestrzeni dyskowej.
37. Wyświetlanie statystyki dotyczącej liczby serwerów, stacji roboczych i wirtualnych maszyn obsługiwanych przez system.

TABELA 1 WYMAGANIA DLA SYSTEMU KOPII ZAPASOWEJ

|  |  |
| --- | --- |
| Lp. | Wymagania ogólne |
|  | Dostarczane licencje muszą zapewniać elastyczność opisaną w punkcie 3 części II oraz zawierać wsparcie producenta na minimum 3 lata. |
|  | Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk produkcyjnych. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: <https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions> |
|  | Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej. |
|  | Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. |
|  | Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. |
|  | Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. |
|  | Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej. |
|  | Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania, dla których nie jest wymagana osobna baza danych z metadanymi deduplikowanych bloków. |
|  | Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-incremental). |
|  | Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji. |
|  | Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. |
|  | Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych do takiej puli. |
|  | Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. |
|  | Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania migawki (snapshota). |
|  | Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji. |
|  | Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji. |
|  | Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania. |
|  | Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX). |
|  | Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej. |
|  | Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie były przekraczane skonfigurowane przez administratora backupu poziomy opóźnień (latencji). Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych. |
|  | Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora. |
|  | Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage. |
|  | Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn. |
|  | Oprogramowanie musi posiadać wsparcie dla NDMP. |
|  | Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son). |
|  | Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC. |
|  | Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. |
|  | Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. |
|  | Repozytoria oparte o XFS muszą pozwalać na niezmienność danych przez określoną ilość czasu (tzw. Immutability) |
|  | Oprogramowanie musi mieć możliwość przesyłania backupów z wykorzystaniem wbudowanej akceleracji WAN dla łączy internetowych o niskiej przepustowości. |
|  | Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków. |
|  | Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2. |
|  | Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików |
|  | Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. |
|  | Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików: * Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
* BSD: UFS, UFS2
* Solaris: ZFS, UFS
* Mac: HFS, HFS+
* Windows: NTFS, FAT, FAT32, ReFS
* Novell OES: NSS
 |
|  | Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). |
|  | Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych. |
|  | Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych. |
|  | Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint. |
|  | Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. |
|  | Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego. |
|  | Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN. |
|  | Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA. |
|  | Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN. |
|  | Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. |
|  | Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem. |
|  | Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. |
|  | Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |
|  | Zamawiający nie wyraża zgody na zaoferowanie oprogramowania o otwartym kodzie źródłowym. Pod pojęciem oprogramowania z otwartym kod źródłowym Zamawiający rozumie oprogramowanie, którego kod źródłowy jest publicznie dostępny. |

Serwer pocztowy

Zamawiający wymaga dostarczenia wszystkich poniższych funkcjonalności w momencie dostarczenia usługi.

|  |  |
| --- | --- |
| **Lp.**  | **Minimalne wymagania**  |
|  | Zamawiający wymaga realizacji zamówienia w postaci usług w chmurze prywatnej.Nie jest dopuszczalna realizacja zamówienia w postaci usługi „w chmurze publicznej”. Wszystkie informacje musza być przechowywane na serwerach dostarczonych w ramach zamówienia. Zamawiający w ramach zamówienia nie dostarcza żadnych zasobów infrastrukturalnych.  |
|  | System powinien zostać dostarczony jako licencje lub subskrypcje, w przypadku modelu subskrypcyjnego konieczne jest dostarczenie 36 miesięcznej subskrypcji. W przypadku licencji, jak i subskrypcji system powinien być objęty wsparciem producenta na warunkach producenta na okres min. 36 miesięcy. |
|  | Zamawiający wymaga aby dostarczony system pocztowy był systemem dedykowanym dla Zamawiającego, to jest: nie współdzielił serwerów aplikacyjnych i/lub bazy danych z innymi podmiotami. |
|  | Zamawiający wymaga dostępności co najmniej **2** TB miejsca na skrzynki pocztowe |
|  | System nie posiada ograniczenia ilości skrzynek pocztowych |
|  | System nie posiada ograniczenia wielkości skrzynki |
|  | System nie posiada ograniczenia wielkości miejsca dla serwera |
|  | System posiada możliwość podpięcia więcej niż jednej domeny  |
|  | System nie posiada konieczności zakupu licencji na dostęp dla użytkownika lub urządzenia klienckiego |
|  | System umożliwia dostęp do serwera poprzez grubego klienta pocztowego (program pocztowy Outlook/Thunderbird i inne) lub cienkiego klienta przeglądarkowego  |
|  | System umożliwia personalizacje strony logowania do systemu pocztowego cienkiego klienta pocztowego |
|  | System umożliwia implementacje zabezpieczeń serwera DKIM, DMARC, SPF. |
|  | System umożliwia odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych.  |
|  | System zapewnia mechanizm powiadomień o dostarczeniu wiadomości do adresata i przeczytaniu wiadomości przez adresata.  |
|  | System umożliwia tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, plikami.  |
|  | System umożliwia zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: kategoryzacja treści, nadawanie ważności |
|  | System posiada wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości (poprzez grubego klienta pocztowego) |
|  | System posiada wsparcie dla klienta poczty elektronicznej MS Outlook 2013 i nowszych wersji.  |
|  | System umożliwia jeden uniwersalny taki sam webowy klient pocztowy na wszystkie posiadane systemy (Win 7, Win 8.1, Mac OS X), niezależny od posiadanego pakietu MS |
|  | System umożliwia udostępnienie usługi POP3, SMTP, IMAP z protokołem TLS do odbioru poczty z zewnątrz  |
|  | System przechowuje skrzynki pocztowe na serwerach w systemie pocztowym  |
|  | System umożliwia integracje z usługa katalogowymi w tym MS Active Directory 2018 i nowsze  |
|  | System posiada funkcjonalność anty-spam umożliwiająca co najmniej:* Automatyczną filtracje spamu wykorzystującą wskazane listy antyspamowe
* System antywirusowy monitorujący pocztę przychodzącą i wychodzącą (wraz z aktualizacją baz)
* Możliwość kwarantanny wiadomości podejrzanych o bycie spamem z możliwością przeglądania i kwalifikacji maili przez administratora oraz użytkownika skrzynki.
* Brak ograniczenia systemu antyspamowego pod względem ilości przetwarzanych maili w czasie
* Możliwość tworzenia białej i zablokowanej listy
* Klasyfikacja wiadomości pod względem spamu poprzez oznaczenia punktowe
* Dostęp do statystyk w postaci wykresów pokazujących co najmniej: ilość maili na minutę, ilość spamu na minutę.
* Dostęp do statystyk przedstawiających: ilość otrzymanych maile w podziale na skrzynkę, wielkość przychodzących i wychodzących, średni czas procesowania jednej wiadomości
 |
|  | System umożliwia udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu. |
|  | System umożliwia podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze. |
|  | System udostępnia mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz lokalizacji, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone. |
|  | System umożliwia tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy |
|  | System posiada mechanizm udostępniania współdzielonych skrzynek pocztowych.  |
|  | System musi umożliwiać tworzenie, obsługę list i grup dystrybucyjnych |
|  | System udostępnia mechanizm automatycznego informowania wewnętrznych i zewnętrznych użytkowników poczty elektronicznej o dostępności lub niedostępności użytkownika.  |
|  | System umożliwia wybór przez użytkownika poziomu szczegółowości udostępnianych informacji o jego dostępności oraz definicje wiadomości zwrotnej. |
|  | Widok rozmowy, automatycznie organizujący wątki wiadomości w oparciu o przebieg wymiany wiadomości między stronami.  |
|  | System posiada mechanizm automatycznego dostosowywania się funkcji wyszukiwania i podpowiadania (przy wybieraniu adresatów listu) kontaktów |
|  | System umożliwia dostęp do poczty elektronicznej i dokumentów przechowywanych w portalu wielofunkcyjnym z poziomu jednego interfejsu zarządzanego przez serwer poczty elektronicznej.  |
|  | System posiada wielofunkcyjną konsole administracyjną umożliwiająca zarządzanie systemem poczty |
|  | System posiada możliwość definiowania (limitu, quoty) na rozmiar skrzynek pocztowych użytkowników. Ponadto zapewniona funkcjonalność informowania użytkownika wykorzystaniu dostępnej dla niego quoty. Ponadto w przypadku przekroczenia quoty informacja zwrotna dla nadawcy wiadomości e-mail. |
|  | System umożliwia definiowanie różnych limitów pojemności skrzynek dla różnych użytkowników. |
|  | System posiada możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone. (poprzez przeglądarkę) |
|  | System posiada możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej.  |
|  | System posiada obsługę interfejsu dostępu do poczty w takich przeglądarkach, jak Chrome, FireFox, Edge, Safari, Opera, Yandex, UC |
|  | Usługa musi być realizowana przez infrastrukturę osadzoną w Centrum Danych spełniające poniższe wymagania:1. Centrum Przetwarzania Danych musi posiadać aktywne elementy infrastruktury IT zapewniające pracę w modelu n+1;
2. Centrum Przetwarzania Danych musi posiadać redundantne wewnętrzne linie dystrybucji energii elektrycznej obsługujące macierze dyskowe;
3. Centrum Przetwarzania Danych musi posiadać redundantne wewnętrzne linie chłodu równolegle obsługujące macierze dyskowe;
4. Centrum Przetwarzania Danych musi posiadać możliwość, aby każdy element linii dystrybucji energii elektrycznej i chłodu mógł być odłączony w celu poddania czynnościom serwisowym bez wpływu na normalną pracę urządzeń dwuzasilaczowych;
5. Centrum Przetwarzania Danych musi posiadać wdrożoną strefową kontrolę dostępu w oparciu o karty zbliżeniowe lub rozwiązanie równoważne;
6. Centrum Przetwarzania Danych musi posiadać całodobową ochronę fizyczną Centrum Przetwarzania Danych z rejestracją kamer na zewnątrz i wewnątrz budynku;
7. Centrum Przetwarzania Danych musi być zlokalizowane na terenie Polski;
8. Centrum Przetwarzania Danych musi posiadać niezależne strefy pożarowe oraz system wczesnej detekcji dymu i ognia, a pomieszczenie kolokacji musi być wyposażone w zautomatyzowaną aparaturę gaśniczą;
9. Centrum Przetwarzania Danych musi mieć zapewnione zasilanie z dwóch niezależnych linii energetycznych oraz rezerwowe zasilanie realizowane przy pomocy UPS oraz minimum jednego agregatu prądotwórczego;
10. Centrum Przetwarzania Danych musi posiadać UPS’y pracujące w nadmiarowej konfiguracji (co najmniej N+1), zapewniając nieprzerwane zasilanie macierzy dyskowej;
11. Centrum Przetwarzania Danych musi pozwalać, aby dystrybucja energii elektrycznej do macierzy dyskowej odbywała się z wykorzystaniem minimum dwóch niezależnych torów zasilania, z minimum jednym torem gwarantowanym (podtrzymanie zasilania z wykorzystaniem UPS i agregatu prądotwórczego);
12. Centrum Przetwarzania Danych musi posiadać Certyfikat Ochrony Elektromagnetycznej wydany przez Agencję Bezpieczeństwa Wewnętrznego.
 |
|  | Zamawiający wymaga instalacji, konfiguracji i utrzymania usługi w trybie 24/7. |
|  | Zamawiający wymaga utrzymywania w ramach usługi backupu danych serwera pocztowego z retencją 7 dni. Zamawiający nie wymaga mechanizmu odtwarzania poszczególnych skrzynek pocztowych użytkownika przy czym powinny być przechowywane co najmniej 2 pełne kopie zapasowe. Dostarczenie systemu backupu leży w gestii Wykonawcy.  |
|  | Zamawiający wymaga migracji kont pocztowych z aktualnie eksploatowanego serwera pocztowego w ilości ok **140** skrzynek pocztowych. |
|  | Zamawiający wymaga zwrotu nienaruszonych i nieuszkodzonych danych po zakończeniu Umowy  |
|  | Świadczona usługa umożliwia przekierowanie ruchu przez urządzenia brzegowe Zamawiającego (w dowolnej konfiguracji) |
|  | Świadczona usługa umożliwia ograniczenia dostępu dla panelu administracyjnego do wskazanych adresów IP lub przez dedykowany tunel VPN. |
|  | Migracja usługi odbędzie się z wykorzystaniem dostępu VPN do serwera pocztowego Zamawiającego. (jeśli wymagane) |
|  | Zamawiający wymaga nadzoru i administracji nad serwerem pocztowym w okresie trwania umowy rozumiany jako: * Zabezpieczenie dostępu do systemu operacyjnego na poziomie fizycznym i systemowym
* Nadzoru nad bezpieczeństwem serwera i reagowanie na incydenty bezpieczeństwa (z wyłączeniem spamu)
* Nadzór nad systemem antyspamowym i antywirusowym
* Zamawiający nie wymaga aby Wykonawca administrował kontami pocztowymi (dodawanie, usuwanie, blokowanie, zmiana hasła)
* Zamawiający wymaga dostępu administracyjnego do serwera pocztowego (konsola administracja dostępna przez WWW z możliwością ograniczenia dostępu poprzez VPN lub do wskazanego adresu IP)
 |