

Opis przedmiotu zamówienia

Rozdział I. Przedmiot zamówienia.

1. Przedmiotem zamówienia jest dostawa licencji w modelu subskrypcyjnym Dynatrace Managed lub licencji równoważnych wraz z gwarancją, zwanych dalej w niniejszym dokumencie „Oprogramowaniem” lub „Subskrybcjami”.
2. Zamawiający wymaga zapewnienia licencji w modelu subskrypcyjnym na okres od dnia podpisania przez Strony protokołu odbioru Oprogramowania (Załącznik nr 2 do Umowy) do dnia 30 maja 2024 roku. Planowany termin podpisania protokołu odbioru Oprogramowania - rozpoczęcia okresu subskrypcji szacuje się na dzień 30.11.2023 r.
3. Zakres przedmiotu zamówienia obejmuje:
 - 1) dostawę licencji do Oprogramowania Dynatrace Managed – zgodnie z wymaganiami zawartymi w **Rozdziale II**, na które składa się:
 - a) 200 sztuk licencji HU,
 - b) 2 mln sztuk licencji typu DEM
 - c) 2 mln sztuk licencji typu DDU,
 - d) 1 mln sztuk licencji typu ASUlub licencji równoważnych spełniających wymagania zawarte w **Rozdziale IV**;
 - 2) świadczenie gwarancji Wykonawcy przez cały okres obowiązywania subskrypcji, zgodnie z wymaganiami zawartymi w **Rozdziale III**.
4. Kryteria stosowane w celu oceny równoważności opisano w **Rozdziale IV**.
5. Zamawiający wykorzystuje aktualnie oprogramowanie Dynatrace Managed, na które składa się:
 - a) 101 sztuk licencji HU,
 - b) 4 sztuki licencji HUH,
 - c) 1 mln sztuk licencji typu DEM,
 - d) 1.2 mln sztuk licencji typu DDU.

Rozdział II. Wymagania w zakresie dostawy i odbioru Oprogramowania:

1. Wykonawca zobowiązuje się do dostawy Oprogramowania, o którym mowa w Rozdziale I pkt 3 ppkt 1 w terminie wskazanym w ofercie złożonej w postępowaniu o udzielenie zamówienie publicznego, nie dłuższym jednak niż do 5 Dni Roboczych od dnia zawarcia Umowy (**termin Dostawy Oprogramowania stanowi kryterium oceny ofert**).
2. Zamawiający dokona odbioru Oprogramowania, polegającym na weryfikacji dostarczonych kluczy licencyjnych, numerów seryjnych oraz dokumentów potwierdzających udzielenie przez producenta Oprogramowania Zamawiającemu licencji, co zostanie potwierdzone Protokołem Odbioru Oprogramowania.
3. Wykonawca zobowiązany jest dostarczyć do biura Zamawiającego przy ul. Świętokrzyska 12 w Warszawie podpisany Protokół Odbioru Oprogramowania w terminie do 3 Dni Roboczych od dnia realizacji dostawy lub w formie elektronicznej na adres e-mail Zamawiającego podpisany elektronicznym podpisem kwalifikowanym.
4. W przypadku zastrzeżeń do realizowanej przez Wykonawcę dostawy Oprogramowania, o której mowa w pkt 1, Zamawiający zgłosi je do Protokołu Odbioru Oprogramowania. Wykonawca zobowiązany jest w terminie do 2 Dni Roboczych od dnia ich otrzymania, do uwzględnienia zgłoszonych zastrzeżeń i ponownego przedstawienia Zamawiającemu do

akceptacji Protokołu Odbioru. W przypadku, o którym mowa w zdaniu poprzednim postanowienia ust. 1 stosuje się odpowiednio jednokrotnie. Brak uwzględnienia we wskazywanym terminie zgłoszonych zastrzeżeń, o których mowa w zdaniu poprzednim stanowi podstawę do uznania dostawy za niewykonaną w terminie umownym.

5. Wykonawca zapewni Zamawiającemu możliwości weryfikacji udzielenia gwarancji Oprogramowania na cały wymagany okres obowiązywania Umowy na etapie odbioru. Brak możliwości weryfikacji udzielenia gwarancji Oprogramowania stanowi podstawę do uznania dostawy za niewykonaną w terminie.
6. W przypadku dostawy oprogramowania równoważnego Wykonawca na etapie odbioru zapewni Zamawiającemu możliwości weryfikacji kompatybilności dostarczonego Oprogramowania z wykorzystywanym przez Zamawiającego. Brak możliwości weryfikacji kompatybilności Oprogramowania stanowi podstawę do uznania dostawy za niewykonaną w terminie.
7. Protokół Odbioru Oprogramowania musi zostać podpisany bez zastrzeżeń przez obie Strony Umowy.

Rozdział III. Wymagania w zakresie gwarancji i rękojmi

1. Wykonawca udziela Zamawiającemu gwarancji, na Oprogramowanie, na okres od dnia podpisania bez zastrzeżeń Protokołu Odbioru Oprogramowania do dnia 30 maja 2024 roku.
2. W ramach gwarancji Wykonawcy, Wykonawca zapewni Zamawiającemu dostęp do serwisu zgłoszeń producenta z możliwością zgłaszania Błędów dotyczących funkcjonowania Oprogramowania. Zamawiający uprawniony jest do zgłaszania Błędów przy użyciu serwisu zgłoszeń lub na adres email lub telefonicznie, w Dni Robocze tj. od poniedziałku do piątku z wyłączeniem sobót, niedziel i dni ustawowo wolnych od pracy w godzinach 8.00-16.00 przez cały okres trwania gwarancji. Dodatkowo Zamawiający wymaga od Wykonawcy obsługi Zgłoszeń, w formie elektronicznej poprzez zapewniony serwis zgłoszeń producenta pod wskazanym adresem www, pocztą elektroniczną lub w formie telefonicznej w godzinach 8.00-16.00 w Dni Robocze tj. od poniedziałku do piątku z wyłączeniem sobót, niedziel i dni ustawowo wolnych od pracy, w języku polskim lub angielskim. Świadczenie pomocy technicznej musi być realizowane bez ograniczeń co do ilości zgłoszeń.
3. Wykonawca jest zobowiązany zapewnić Zamawiającemu dostęp do strony internetowej WWW producenta Oprogramowania, zawierającej odpowiednie pliki do pobrania, zawierające poprawki, aktualizacje, nowe wersje Oprogramowania, wykaz znanych symptomów i rozwiązań, biuletynów technicznych, dokumentacji technicznych aktualizacji w języku polskim lub angielskim, oraz bazy danych zgłoszonych problemów technicznych przez 24 godziny na dobę, 7 dni w tygodniu — pod wskazanym przez Wykonawcę adresem internetowym niezwłocznie po ich udostępnieniu na stronie Producenta Oprogramowania. W przypadku wystąpienia trudności w związku z instalacją poprawek, aktualizacji, nowych wersji Oprogramowania, o których mowa powyżej, Wykonawca zobowiązuje się do wsparcia Zamawiającego w sposób określony w pkt 4. W przypadku braku możliwości pobrania plików ze wskazanej strony internetowej, Wykonawca jest zobowiązany na każde żądanie Zamawiającego do dostarczenia poprawek/aktualizacji/nowych wersji Oprogramowania, na elektronicznych nośnikach informacji w terminie 5 Dni Roboczych od dnia zgłoszenia takiego żądania, co zostanie potwierdzone Protokołem Przekazania Nośnika (Załącznik nr 7) do Umowy). Żądanie Zamawiający składa w formie elektronicznej na adres mail lub telefonicznie – wg danych wskazanych e w Umowie.

4. W przypadku nieprawidłowego działania Oprogramowania Wykonawca po otrzymaniu Zgłoszenia Błędu musi zagwarantować:
- 1) Czas Reakcji na Zgłoszenie, który nie będzie dłuższy niż:
 - a) dla Zgłoszeń Błędu o Krytycznym Priorytecie – 4 godziny,
 - b) dla Zgłoszeń Błędu o Wysokim Priorytecie – 1 Dzień Roboczy,
 - c) dla Zgłoszeń Błędu o Średnim Priorytecie – 2 Dni Robocze,
 - d) Zgłoszeń Błędu o Niskim Priorytecie – 4 Dni Robocze.
 - 2) W Czasie Reakcji Wykonawca potwierdza przyjęcia Zgłoszenia Błędu i zdiagnozowanie Błędu. Wykonawca zobowiązany jest do niezwłocznego podjęcia wszelkich niezbędnych działań zmierzających do usunięcia Błędu i przywrócenia w pełni prawidłowego działania Oprogramowania.
 - 3) Przez Zgłoszenie Błędu rozumie się poinformowanie Wykonawcy o zaistniałym Błędzie przez Zamawiającego lub innego upoważnionego przez niego przedstawiciela przez uzgodniony kanał komunikacji (np. drogą elektroniczną).
 - 4) Wykonawca zobowiązany jest do usunięcia zgłoszonego Błędu w terminie, który nie może być dłuższy niż:
 - a) dla Zgłoszeń Błędu o Krytycznym Priorytecie – 1 Dzień Roboczy,
 - b) dla Zgłoszeń Błędu o Wysokim Priorytecie – 5 Dni Roboczych,
 - c) dla zgłoszeń Błędu o Średnim Priorytecie – 10 Dni Roboczych,
 - d) dla zgłoszeń Błędu o Niskim Priorytecie – 15 Dni Roboczych,- od dnia potwierdzenia przyjęcia Zgłoszenia Błędu i zdiagnozowania Błędu.
 - 5) Formularz Zgłoszenia Błędu (Załącznik nr 8 do Umowy) przesłany przez Zamawiającego stanowi formalne potwierdzenie Zgłoszenia Błędu i od momentu potwierdzenia jego przyjęcia przez Wykonawcę biegnie odpowiedni termin rozwiązania Zgłoszenia Błędu;
 - 6) W sytuacjach, gdy Wykonawca nie jest w stanie rozwiązać Zgłoszenia w terminie realizacji danego Zgłoszenia, Wykonawca przed upływem terminu realizacji danego Zgłoszenia może wystąpić z wnioskiem do Zamawiającego na adres e-mail wskazany w § 12 ust. 1 pkt 1 Umowy, o przedłużeniu tego terminu wraz z propozycją nowego terminu rozwiązania Zgłoszenia Błędu. Przedstawiciel Zamawiającego, na podstawie prawidłowo złożonego przez Wykonawcę wniosku wraz z uzasadnieniem, może przedłużyć termin realizacji Zgłoszenia, co zostanie potwierdzone e-mailem na adres, o którym mowa w § 12 ust. 2 Umowy.
 - 7) Wykonawca po rozwiązaniu Zgłoszenia Błędu poinformuje o tym Zamawiającego na adres e-mail, o którym mowa w § 12 ust. 1 pkt 1 Umowy wraz z opisem sposobu rozwiązania Błędu. Zamawiający zastrzega prawo do weryfikacji rozwiązania Błędu oraz do zgłoszenia reklamacji w serwisie zgłoszeń producenta.

Rozdział IV. Opis wymagań w zakresie produktów równoważnych:

1. Opis równoważności dla funkcjonalności - dotyczący typu licencji:
 - a) licencja równoważna do HU to taka, która pozwala na monitorowanie całego stosu technologicznego lub samej infrastruktury dla wybranego hosta, nie ograniczona pod względem ilości zebranych danych jak i czasu kolekcjonowania metryk. Konsumpcja jednostek równoważnych do HU musi umożliwiać monitorowanie pełnego stosu technologicznego („full-stack”) na hoście i tak być licencjonowana aby dla rozmiaru pamięci

RAM monitorowanego hosta i dla trybu „Full-Stack” była wyrażona co najwyżej krotnością 16G zaokrągloną do góry bez względu na liczbę CPU czy liczbę monitorowanych technologii na hoście. W przypadku trybu „Infrastructure” konsumpcja jednostek HU musi wynosić co najwyżej 0.03 HU dla 1.6GiB i mniej, 0.75 HU dla 4GiB i mniej, 0.15 HU dla 8 GiB i mniej, 0.3 HU dla 16 GiB i mniej, 0.6 dla 32 GiB i mniej, 0.9 dla 48 GiB i mniej, 1 dla więcej niż 48 GiB;

- b) licencja równoważna do HUH to rozszerzenie pojęcia licencji HU o konsumpcję jednostki HU w określonym przedziale czasu. 1 host unit hours overage odpowiada 1 jednostce HU zużywanej przez 1 godzinę. Na 1 sztukę licencji HUH przypada 9k jednostek host unit hours overage;
 - c) licencja równoważna do DEM to taka, która rozszerza możliwość Oprogramowania o monitorowanie odczuć cyfrowych użytkownika końcowego i opiera się między innymi na RUM (ang. Real User Monitoring), EUM (End User Monitoring) oraz SM (ang. Synthetic Monitoring). Konsumpcja jednostek DEM bazuje na sesjach użytkowników lub w przypadku SM na żądaniach wywołania HTTP. Pojedyncza, 60-minutowa sesja dla monitorowania RUM zużywa co najwyżej 0.25 DEM. Monitorowanie syntetyczne konsumuje co najwyżej 1 DEM na jedno wykonanie;
 - d) licencja równoważna do DDU to taka, która rozszerza możliwość Oprogramowania o śledzenie logów, zbieranie niestandardowych metryk. Konsumpcja jednostek DDU w przypadku zbierania logów opiera się o zliczanie wszystkich przychodzących rekordów dziennika. Każdy rekord dziennika (wiersz, wiadomość, wpis) konsumuje co najwyżej 0.0005 DDU. , natomiast w przypadku zbierania danych z metryk niestandardowych co najwyżej 0.001 DDU na metrykę;
 - e) licencja równoważna do ASU to taka, która rozszerza możliwość Oprogramowania o monitorowanie bezpieczeństwa aplikacji, które pozwalają wizualizować, analizować i monitorować podatności w zabezpieczonych środowiskach, które są powiązane z dodatkowymi bibliotekami wykorzystywanymi podczas wykonywania kodu aplikacji. Konsumpcja jednostek równoważnych do ASU musi być wyrażona co najwyżej krotnością 16GiB pamięci RAM, zaokrągloną do góry dla przypadku gdy zabezpieczenie polega tylko na analizie podatności zabezpieczanego środowiska – zabezpieczenie podstawowe, a w przypadku gdy zabezpieczenie polega dodatkowo na ochronie aplikacji w czasie rzeczywistym konsumpcja jednostek ASU stanowi co najwyżej podwojenie zużycia jednostek jak dla zabezpieczenia podstawowego.
2. Dostarczone oprogramowanie równoważne musi należeć do klasy oprogramowania typu APM (ang. Application Performance Monitoring).
 3. Dostarczone Oprogramowanie musi być w pełni kompatybilne z oprogramowaniem aktualnie wykorzystywanym przez Zamawiającego wskazanym w Rozdziale I pkt 5.
 4. Dostarczone Oprogramowanie musi zapewniać instalację części centralnej w infrastrukturze Zamawiającego jako maszyny wirtualne w takich środowiskach Zamawiającego jak VmWare. Niedopuszczalne są rozwiązania instalowane poza lokalizacją Zamawiającego.
 5. Oprogramowanie dostarczone przez Wykonawcę ma zapewnić monitorowanie środowiska Zamawiającego. Musi zapewnić monitorowanie wydajności i sprawności środowiska teleinformatycznego Zamawiającego, a raporty mają być dostępne dla obsługujących oprogramowanie administratorów oraz tzw. biznesu w formie czytelnych raportów, np. z niedostępności danej usługi.

6. Oprogramowanie musi umożliwiać maskowanie danych, nazw operacji w czasie rzeczywistym (natychmiastowo) definiowanych/wskazanych przez administratora systemu np. adresy IP.
7. Oprogramowanie musi zapewniać, aby dostęp do oprogramowania był zabezpieczony hasłem.
8. Oprogramowanie musi pozwalać na zabezpieczenie dostępu z poziomu operatora i użytkownika oprogramowania za pomocą protokołu HTTPS.
9. Dostarczone w ramach usługi licencje do Oprogramowania muszą być przenaszalne między środowiskami i serwerami.
10. Rozwiązanie i model licencjonowania muszą uwzględniać możliwość czasowego skalowania środowiska po stronie zamawiającego, np. chwilowy up-scaling wynikający z większego zapotrzebowania na moc obliczeniową.
11. Dostarczone Oprogramowanie do monitoringu nie może ograniczać liczby użytkowników końcowych korzystających z Oprogramowania.
12. Dla oferowanego Oprogramowania musi istnieć wsparcie w języku polskim i angielskim.
13. Oferowane Oprogramowanie powinno być opisane na publicznie i powszechnie dostępnych stronach WWW producenta lub społeczności rozwijającej produkt.
14. Wszystkie komponenty oferowanego Oprogramowania powinny być gotowe w momencie złożenia oferty.
15. Wszystkie komponenty Oprogramowania muszą posiadać gotową w momencie złożenia oferty dokumentację w języku polskim lub angielskim. Dokumentacja powinna być publicznie i powszechnie dostępna w momencie złożenia oferty.
16. Oprogramowanie musi posiadać możliwość uruchomienia monitoringu dla aplikacji pracujących przynajmniej na:
 - a) na platformach sprzętowych: Intel lub AMD x86_64,
 - b) systemach operacyjnych: Linux x86_64 lub Windows Server 2008+ R2.
17. Elementy oferowanego rozwiązania muszą w zakresie komunikacji (wewnętrznej i zewnętrznej) wykorzystywać protokoły SSL/TLS.
18. Oprogramowanie powinno zapewniać mechanizm równoważenia obciążenia oraz zapewnienia redundancji elementów zbierających dane od agentów aplikacyjnych (kolektory danych). Dodawanie kolejnych kolektorów do grupy LB powinno następować automatycznie, bez konieczności restartów agenta monitorującego oraz systemu monitorowanego.
19. Aktualizacje oprogramowania muszą mieć możliwość automatycznego pobierania na serwer. Administrator musi mieć możliwość ustawienia automatycznego lub ręcznego sposobu instalowania aktualizacji. Aktualizacja musi być wykonywana z poziomu centralnej konsoli serwera bez konieczności ręcznej aktualizacji poszczególnych komponentów takich jak agenci serwerowi, kolektory zbierające dane oraz serwery oprogramowania monitorującego.
20. Oprogramowanie musi:
 - a) monitorować wielowarstwowe aplikacje wykonanych co najmniej w technologii Java, PHP, .Net działające na serwerach aplikacyjnych używanych przez Zamawiającego co najmniej: Apache, Nginx, JBoss, WebSphere, WildFly, Weblogic, Tomcat, IIS oraz innych zgodnych z technologią J2EE, a także aplikacje oparte o WCF.
 - b) wykrywać i monitorować przebieg wszystkich transakcji przez aplikację bez potrzeby definiowania zależności pomiędzy warstwami; tak wykryte przebiegi mają być prezentowane w formie graficznej w celu ich łatwej analizy, z uwzględnieniem warstw takich jak serwery WWW, aplikacyjne, bazodanowe, aplikacje klienckie (przeglądarka, urządzenie mobilne)

- c) wytworzyć linie bazowe dla monitorowanych transakcji biznesowych, które będą adaptowały się względem charakterystyki pracy aplikacji - oprogramowanie musi automatycznie wyliczać parametry typu czas odpowiedzi oraz procent błędów, które są typowe dla aplikacji i generować alerty tylko w razie przekroczenia wartości "normalnych". Operator musi mieć możliwość określenia dopuszczalnych poziomów odstępstw od normy na poziomie wartości lub procentu odchylenia lub sztywnych progów
- d) monitorować i śledzić przebieg wszystkich wykonywanych transakcji pomiędzy wszystkimi warstwami aplikacji w środowisku z możliwością uzyskania następujących informacji o każdej z pojedynczych transakcji:
- e) drzewo wywołania kodu oprogramowania w ramach ścieżki wykonania – do poziomu nazwy wywoływanej metody, zarówno dla wątków wywoływanych synchronicznie jak i asynchronicznie
- f) czasach odpowiedzi serwera do aplikacji klienckiej jak i całkowitym czasie wykonania transakcji po stronie serwera (wątków synchronicznych oraz asynchronicznych)
- g) czasy wykonania pojedynczych metod,
- h) zapytań SQL wykonanych w ramach transakcji z możliwością uzyskania informacji o tzw. bind variables (zmiennych wiązanych),
- i) wartość parametrów wywołania wskazanych metod,
- j) wartości zwracanych przez wskazane metody.
- k) zbierać i monitorować wszystkie zapytania SQL wykonywane z poziomu monitorowanej aplikacji z możliwością ich powiązania z transakcjami, które dane zapytania wykonują,
- l) monitorować serwery webowe w zakresie wprowadzanych przez nie opóźnień w czasie realizacji transakcji webowej oraz błędów pojawiających się na tychże serwerach,
- m) Agent lub kolektor danych powinien kontrolować overheads jaki generuje i w przypadku zwiększonego narzutu automatycznie ograniczać ten narzut
- n) posiadać możliwość prezentowania na wykresach dowolnych, konfigurowalnych wartości z transakcji biznesowych dla zaobserwowanych przepływów transakcyjnych,
- o) wspierać gromadzenie danych zagregowanych o czasach przetwarzania na potrzeby wykonywania raportów co najmniej SLA,
- p) pozwalać na tworzenie dowolnych niestandardowych wykresów i pulpitów nawigacyjnych, do których mogą być dowolnie definiowane uprawnienia dla użytkowników rozwiązania APM, co oznacza, że Oprogramowanie musi udostępniać interfejs graficzny pozwalający na definiowanie niestandardowych wykresów i pulpitów nawigacyjnych prezentujących wszelkie gromadzone przez oprogramowanie dane. Oprogramowanie musi umożliwiać nadawanie użytkownikom uprawnień do poziomu poszczególnego wykresu/uprawnienia.
- q) umożliwiać tworzenie sekwencji UML dla każdej, pojedynczej transakcji,
- r) umożliwiać analizę użycia pamięci aplikacji na poziomie zrzutu ze sterty Java, pozwalająca śledzić obiekty wywoływane i wywołujące, powiązania między nimi, wielkość pamięci alokowaną przez poszczególne obiekty i wielkości tych obiektów,
- s) mechanizmy bezpieczeństwa w zakresie dostępu do zbieranych danych, narzędzie musi gwarantować odpowiedni poziom dostępu do danych definiowany na poziomie nadawania uprawnień w aplikacji do monitorowania.
- t) umożliwiać wyodrębnienie i oddzielną prezentację ruchu, czy przebiegu sesji pochodzących od różnych aplikacji oraz umożliwi własną definicję aplikacji.
- u) umożliwiać porównywanie działania aplikacji dla różnych wydań i wskazania różnic w działaniu oprogramowania aż do poziomu metod i API.
- v) umożliwiać integrację z CMDB wykorzystywaną przez Zamawiającego.

- w) Oprogramowanie ma wspierać śledzenie wszystkich transakcji pomiędzy różnymi aplikacjami, które wykorzystują co najmniej następujące technologie synchroniczne i asynchroniczne:
 - i) http
 - ii) REST
 - iii) SOAP/XML
 - iv) JMS
 - v) WCF
 - vi) MQTT
 - x) Oprogramowanie musi wspierać definiowanie transakcji biznesowej na podstawie dowolnych kryteriów, np.:
 - i) URL
 - ii) Wartość parametru z nagłówka http
 - iii) Wartość parametru z zapytania GET lub POST
 - iv) Wartość atrybutu sesji http
 - v) Wykonanie konkretnej metody w kodzie Java, .NET, PHP, NodeJS
 - vi) Wykonanie konkretnego zapytania SQL
 - vii) Wywołanie konkretnej usługi Webservice
21. Oprogramowanie ma umożliwiać definiowanie raportów wg predefiniowanych kryteriów wyszukiwania w postaci tabelarycznej lub graficznej z całego zakresu danych jakie gromadzi. Oprogramowanie musi zapewniać możliwość ręcznego i automatycznego generowania raportów (przynajmniej w formacie PDF) oraz zapisywania ich na dysku lub wysłania przy pomocy wiadomości email.
22. Oprogramowanie musi być rozwiązaniem typu full-stack i umożliwiać monitoring podstawowych parametrów infrastruktury (CPU, pamięć, zajętość dysków, użycie interfejsów sieciowych, pliki dziennika), komponentów środowiska aplikacyjnego.
23. Oprogramowanie musi zbierać informacje o wszystkich wyjątkach, błędach http oraz wpisach do logów. Musi istnieć możliwość zobaczenia szczegółowych informacji na temat transakcji, które wygenerowały wyjątek albo wpis do logu. Wymaganie musi być spełnione dla logów typu:
- a) WARNING
 - b) ERROR
 - c) SEVERE
 - d) FATAL
24. Oprogramowanie musi umożliwiać monitoring błędów po stronie przeglądarki (np. błędy JavaScript) lub urządzenia mobilnego.
25. Oprogramowanie ma umożliwiać korelację wszystkich działań użytkownika na stronie WWW – dla każdej interakcji i każdej wizyty, co umożliwi znalezienie każdego użytkownika i diagnostykę jego interakcji z systemem.
26. Oprogramowanie musi umożliwiać powiązanie każdej wizyty z interakcją z systemem i transakcjami realizowanymi przez system na poziomie sekwencji wywołanych metod i skorelowanych informacji infrastrukturalnych, end-2-end, od kliknięcia w stronę lub aplikację mobilną, poprzez serwery www, aplikacyjne aż do odpowiedzi z bazy danych. Wymaganie dla systemów WWW oraz klientów mobilnych musi być spełnione bez potrzeby zmiany kodu źródłowego aplikacji.
27. Oprogramowanie ma umożliwiać monitorowanie każdej interakcji użytkownika na poziomie aplikacji www, aplikacji mobilnej czy grubego klienta – z zachowaniem tej samej perspektywy UEM (ang. User Experience Management) i tego samego zunifikowanego podejścia. Jeśli strona www zawiera w sobie np. aplet, może on być także objęty monitorowaniem UEM i być

włączony do zestawu informacji nt. interakcji użytkownika z systemem /wizyta użytkownika/. Prezentowanie informacji muszą uwzględniać czas spędzony po stronie serwera, stacji klienckiej, sieci dla każdego wywołania i grup wywołań użytkowników końcowych. Wymaganie dla systemów WWW oraz klientów mobilnych musi być spełnione bez potrzeby zmiany kodu źródłowego aplikacji.

28. Monitorowanie pracy i doświadczeń użytkownika końcowego (ang. user experience) nie może wymagać instalacji dodatkowych komponentów po stronie użytkownika i nie powinno wymagać zmian konfiguracji serwerów WWW lub aplikacyjnych. Zmiana konfiguracji czy też włączenie/wyłączenie monitorowania odczuć użytkownika powinno odbywać się z konsoli narzędzia, bez potrzeby restartu serwerów monitorowanego środowiska. Wymaganie dla systemów WWW oraz klientów mobilnych musi być spełnione bez potrzeby zmiany kodu źródłowego aplikacji.
29. Oprogramowanie musi umożliwiać dla każdego rodzaju interakcji zbieranie metryk, także biznesowych, pozwalających na ocenę jak poszczególne kanały interakcji /mobilne, www, itp./ wykorzystywane są do realizacji zadań biznesowych. Dane te powinny zapewniać możliwość opracowania zestawień statystycznych dotyczących między innymi czasu spędzanego w poszczególnych elementach formularza, map przejścia procesów biznesowych itd. Zagregowane dane powinny umożliwić identyfikację obszarów aplikacji, których obsługa trwa najdłużej. Źródłem danych do zbieranych metryk biznesowych mogą być m.in. wartości tagów HTML, atrybuty elementów, selektory css, zmienne JavaScript, metadane.
30. Oprogramowanie ma umożliwiać dostarczanie informacji nt. charakteru każdej interakcji w systemie dla każdego pojedynczego użytkownika ze wskazaniem np. na landing pages, exit pages, wpływ third party czy ładowania asynchroniczne AJAX. Wymaganie dla systemów WWW oraz klientów mobilnych musi być spełnione bez potrzeby zmiany kodu źródłowego aplikacji.
31. Licencje wymagane do pracy oprogramowania muszą pracować w trybie „pływającym” (ang. floating licenses), co oznacza możliwość niejednoczesnego wykorzystania ich w wielu systemach jednocześnie. W takim wypadku systemy, niemonitorowane, pomimo zainstalowania oprogramowania monitorującego (np. agenta), nie zużywają licencji. Oprogramowanie centralne powinno umożliwiać centralne zarządzanie wyłączaniem (i zwalnianiem licencji) monitoringu dla systemów gdzie takie monitorowanie ma być wstrzymane.
32. Oprogramowanie musi zapewniać przenaszalność licencji między środowiskami (o tożsamy parametrach) objętymi systemem monitorowania bez konieczności wykupywania dodatkowych licencji.
33. Dostarczane licencje nie mogą ograniczać liczby monitorowanych procesów JAVA na JVM oraz .NET działających w środowisku, dla którego uruchomiono agenta monitorującego.
34. Oprogramowanie domyślnie nie może być limitowany na ilość zdarzeń w czasie. Oznacza to, że w danym czasie może wpłynąć dowolna ilość zdarzeń i muszą one zostać zarejestrowane przez Oprogramowanie.
35. Oprogramowanie musi umożliwiać dostęp do logów aplikacyjnych i systemowych, przeszukiwanie ich i przeglądanie bez konieczności logowania na serwer monitorowany,
36. Oprogramowanie musi zapewniać równoczesną, niezakłóconą pracę wielu użytkowników (minimum 100), posiadających własne loginy i hasła.
37. Oprogramowanie musi zapewniać możliwość prezentowania na wykresach danych wzorcowych (metryk) które przechowuje i umieszczać je w interfejsach graficznych, prezentujących informacje, musi zapewnić dowolność w wyborze tych danych nie ograniczając się do jednej metryki.

38. Oprogramowanie musi zapewniać prognozowanie wartości danych dotyczących monitorowanej infrastruktury w przyszłości, za wybrany okres czasu.
39. Oprogramowanie musi posiadać wbudowaną funkcjonalność nauczania maszynowego do celów predykcji wartości badanych parametrów. W szczególności oprogramowanie musi posiadać możliwość stosowania algorytmów nauczania takich jak: sieć neuronowa, zmienne drzewa decyzyjne, regresja liniowa.
40. Oprogramowanie musi być wspomagane uczeniem maszynowym w badaniu korelacji między zbieranymi metrykami w celu wykrywania problemów i związków przyczynowo skutkowych które prawdopodobnie doprowadziły do pojawienia się np. spadku wydajności aplikacji.
41. 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.
42. Oprogramowanie musi umożliwiać korelację transakcji realizowanych przez monitorowane komponenty z odpowiadającymi im danymi infrastrukturalnymi, bazodanowymi, mechanizmami sesji.
43. Oprogramowanie musi automatycznie, na podstawie danych bazowych/wzorcowych wykrywać problemy związane co najmniej z:
 - a) wydłużeniem czasów odpowiedzi poszczególnych usług po stronie serwerowej,
 - b) zwiększeniem poziomu problemów dla poszczególnych usług po stronie serwerowej,
 - c) wydłużeniem czasów odpowiedzi dla poszczególnych akcji wykonywanych przez użytkownika końcowego na aplikacji WWW lub aplikacji mobilnej,
 - d) zwiększeniem poziomu problemów (w tym błędów JavaScript) dla poszczególnych akcji wykonywanych przez użytkownika końcowego na aplikacji WWW lub aplikacji mobilnej,
 - e) przeciążeniem CPU,
 - f) nadmiernym wykorzystaniem pamięci,
 - g) spadkiem wydajności dysków,
 - h) dostępnością na warstwie TCP,
 - i) wzrostem liczby zgubionych pakietów (w powiązaniu interfejsu sieciowego z danym procesem),
 - j) spadkiem ruchu w aplikacjach lub usługach (zmniejszenie liczby wywołań),
 - k) brakiem dostępności aplikacji,
44. Oprogramowanie musi zapewniać porównywanie działania tej samej aplikacji w różnych przedziałach czasowych w zakresie co najmniej: czasów odpowiedzi, liczby wykrytych problemów oraz wykrytych elementów krytycznych infrastruktury Zamawiającego, mających największy udział w czasach wykonania (np. czas wywołania usług zewnętrznych, czas odpowiedzi bazy danych, czas sieci).
45. Oprogramowanie musi umożliwiać monitoring połączeń między poszczególnymi serwerami i procesami, w monitorowanej infrastrukturze i udostępniać automatycznie budowaną mapę połączeń w formie graficznej. W przypadku wykrycia odstępstwa od normy skutkującej wygenerowaniem alertu, serwer oraz proces, muszą zostać oznaczone na wizualizacji w sposób jednoznacznie wskazujący na wystąpienie problemu.
46. Oprogramowanie musi przeciwdziałać multiplikowaniu alarmów dotyczących tego samego problemu i grupować je na podstawie zależności między serwerami, procesami i usługami oraz posiadać mechanizmy konfigurowania zasad eskalacji. Przykład – jeżeli wykryte zostanie przeciążenie CPU na serwerze aplikacyjnym i wzrosną czasy odpowiedzi tego serwera to system musi zaraportować jeden alarm łączący oba zdarzenia zamiast dwóch niezależnych.

47. Oprogramowanie musi w przypadku wykrycia problemu automatycznie wskazać najbardziej prawdopodobną przyczynę wystąpienia problemu.
48. Oprogramowanie musi umożliwiać definiowanie alarmów na podstawie wykrycia problemów w logach systemu operacyjnego lub monitorowanych aplikacji.
49. Oprogramowanie musi zapewniać gromadzenie i dostęp do danych dotyczących wykrytych problemów, po stronie przeglądarki (np. błędy JavaScript) lub urządzenia mobilnego.
50. Oprogramowanie musi posiadać mechanizm nadawania uprawnień i tworzenia ról dla poszczególnych elementów oprogramowania i użytkowników, tak aby można było udostępniać dane jedynie dla wybranych elementów architektury (pojedyncze serwery i procesy) i dla poszczególnych środowisk oraz ograniczyć dostęp użytkowników do poszczególnych zgromadzonych danych. Oprogramowanie musi mieć wprowadzony mechanizm bezpieczeństwa, który kontroluje jaki użytkownik ma dostęp do jakiego fragmentu danych. Mechanizm konfiguracji uprawnień musi być dostępny w poziomie www aplikacji jak i z API. Wprowadzone ograniczenia dostępu muszą pracować jednolicie dla operacji wyszukiwania danych z GUI jak i z poziomu API.
51. Oprogramowanie musi logować wszystkie aktywności użytkowników związane ze zmianami konfiguracji. Logowanie musi umożliwiać jednoznaczne wskazanie osoby, która wykonała zmianę.
52. Oprogramowanie musi zapewniać zbieranie danych wyodrębnianych z plików logów umieszczonych w wyszczególnionym katalogu na serwerze z systemem.
53. Oprogramowanie musi zapewniać indeksowanie i przetwarzanie nieokreślonej liczby zdarzeń w ramach wydajności pojedynczego serwera, na którym pracuje. Retencja danych powinna być konfigurowalna.
54. Oprogramowanie musi zapewniać odczyt i analizę (ang. parsing) przesyłanych danych z logów (systemowych, aplikacyjnych).
55. Oprogramowanie musi zapewniać rozpoznanie formatów czasu i daty w przetwarzanych danych z logów i normalizowanie ich do jednego wspólnego formatu.
56. Oprogramowanie musi zapewniać użytkownikowi posiadającemu uprawnienia samodzielne konfigurowanie reguł odczytu i analizowania (ang. parsing) nierozpoznanych przez oprogramowanie formatów logów w celu umożliwienia analizy zebranych w nich informacji.
57. Oprogramowanie musi być obsługiwany z poziomu przeglądarki internetowej.
58. Oprogramowanie musi zapewniać wyszukiwanie w całym zgromadzonym przez niego zbiorze danych wg dowolnych filtrów. Musi istnieć możliwość wyszukiwania na podstawie jednoczesnego wykorzystania więcej niż jednego zdefiniowanego przez użytkownika wzorca wyszukiwania.
59. Oprogramowanie musi pozwalać na użycie operatorów logicznych, wzorców, wyrażeń regularnych (REGEX) do przeszukiwania danych.
60. Oprogramowanie musi pozwalać na geolokalizację zdarzeń na bazie adresów IP oraz umożliwiać jej wizualizację na mapie.
61. Oprogramowanie musi pozwalać na wprowadzenie mapowania danych geolokalizacyjnych dla wewnętrznej adresacji IP poprzez wprowadzenie wymaganych danych przez interface web lub plik CSV.
62. Oprogramowanie musi działać proaktywnie i automatycznie wykrywać stos technologiczny na maszynie, która objęta jest monitoringiem.
63. Oprogramowanie musi mieć możliwość integracji z aplikacjami open source używanymi do monitorowania infrastruktury, tj. Logstash, Prometheus, Zabbix, Nagios.
64. Oprogramowanie musi umożliwiać monitoring aplikacji uruchamianych w środowisku skonteneryzowanym (co najmniej Docker) na poziomie zarówno pojedynczych kontenerów jak

- i serwera, na którym są uruchamiane. Konfiguracja monitoringu musi być zautomatyzowana, bez konieczności konfigurowania poszczególnych obrazów kontenerów.
65. Oprogramowanie musi umożliwiać monitoring serwerów w centrach danych chmurowych (co najmniej AZURE).
 66. Oprogramowanie musi być dostarczone wraz z wszystkimi komponentami koniecznymi do jego uruchomienia, działania i korzystania z wszystkich wymienionych i opisanych w tym dokumencie funkcjonalności ograniczonymi jedynie warunkami licencyjnymi producenta.
 67. Oprogramowanie musi zapewniać mechanizm równoważenia obciążenia oraz zapewnienia redundancji części serwerowej w obszarze aplikacji oraz bazy danych jak i elementów zbierających dane od agentów aplikacyjnych. Dodawanie kolejnych elementów Oprogramowania musi następować automatycznie, bez konieczności restartów Oprogramowania monitorującego oraz systemu monitorowanego i nie wymagać od Zamawiającego zakupu dodatkowej licencji na oprogramowanie oraz bazę danych.
 68. Wszystkie funkcjonalności Oprogramowania muszą być dostarczone w ramach licencji, które nie mogą powodować konfliktów pomiędzy danymi jego częściami oraz powodować negatywnych skutków prawnych i funkcjonalnych dla Zamawiającego.
 69. Oprogramowanie musi posiadać interfejs do tworzenia lub konfigurowania definiowanych przez administratora aplikacji dodatkowych wtyczek monitorujących.
 70. Oprogramowanie musi umożliwiać monitorowanie serwerów baz danych zarówno relacyjnych jak i nie relacyjnych w tym zbierać przynajmniej metryki takie jak czasy wykonywania zapytań, konsumpcji zasobów (pamięć, I/O, CPU) w przypadku baz transakcyjnych zbierać przynajmniej dane o najdłużej wykonujących się transakcjach, transakcjach blokujących, mieć możliwość grupowania najczęściej wykonujących się zapytań.
 71. Oprogramowanie musi umożliwiać wysyłanie powiadomień o wystąpieniu problemów do aplikacji np.: Jira Service Desk, Service Now, Slack, Trello, Email.
 72. Oprogramowanie musi umożliwiać zdefiniowanie własnej integracji http (payload JSON) pozwalającej na wysyłanie powiadomień o problemach do innych rozwiązań.
 73. Oprogramowanie musi umożliwiać integrację bazy użytkowników z LDAP.
 74. Oprogramowanie musi umożliwiać integrację poświadczeń użytkowników poprzez interfejs SAML 2.0
 75. Oferowane rozwiązanie musi posiadać komercyjne wsparcie producenta i jego inżynierów w ramach oferowanej licencji. Wykluczone jest oferowanie rozwiązania, którego wsparcie oparte jest tylko na wsparciu społeczności użytkowników.
 76. Oprogramowanie musi posiadać moduł bezpieczeństwa pozwalający na weryfikację podatności w użytych bibliotekach oraz ochronę aplikacji w czasie rzeczywistym dla technologii Java, .NET, PHP, NodeJS zarówno przy instalacjach klasycznych jak i deployment na Kubernetes. Funkcjonalność musi być realizowana przez tych samych agentów, którzy służą do monitoringu systemu.
 77. Oprogramowanie musi oferować także udokumentowany interfejs programistyczny (API) służący do przeszukiwania danych historycznych
 78. Oprogramowanie musi mieć możliwość symulowania syntetycznego użytkownika aplikacji Zamawiającego, z uwzględnieniem czasów wykonania transakcji logicznych/biznesowych. Automatycznie stworzony scenariusz (skrypt) musi mieć możliwość edycji i parametryzowania.
 79. Oprogramowanie nie może wymagać aby do monitorowania aplikacji Zamawiającego konieczne były zmiany w samej aplikacji Zamawiającego np. poprzez dołączenie dodatkowych bibliotek zarówno po stronie aplikacji jak i serwera aplikacji na którym ta aplikacja jest osadzona. Czyli dopuszczalne jest instalowanie agentów, kolektorów danych na systemie operacyjnym serwera aplikacji, który będzie monitorowany, ale nie dopuszczalne jest

rozwiązanie, które wymagać będzie zmian na serwerze aplikacyjnym np. JBoss, Wildfly poprzez dołączenie dodatkowych bibliotek.

80. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego.
81. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty wsparcia technicznego bądź gwarancji producentów oprogramowania używanego przez Zamawiającego, w szczególności wykorzystywanych aplikacji dziedzinowych.
82. W przypadku gdy oferowane Oprogramowanie równoważne będzie wymagało dodatkowych licencji niezbędnych do jego uruchomienia Wykonawca zobowiązany jest dostarczyć je na swój koszt.
83. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat, licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.
84. Wykonawca dostarczy, udostępni lub wskaże na publicznie dostępnych zasobach dokumentację administratora oprogramowania zawierającą opis instalacji i konfiguracji oprogramowania, interfejsu oprogramowania oraz sposób wykorzystania funkcji oprogramowania. Dokumentacja musi być dostępna w języku polskim lub angielskim.
85. Pozostałe wymagania dotyczące oprogramowania równoważnego:
 1. Zamawiający może swobodnie przenosić usługę monitorowania między serwerami w ramach dostarczonego przez Wykonawcę limitu wynikającego z zamówionych Subskrypcji.
 2. W przypadku dostarczenia Oprogramowania równoważnego Wykonawca zobowiązany jest do przeprowadzenia instalacji i konfiguracji zgodnie z wymogami z niniejszego Rozdziału.
 3. W przypadku dostarczenia licencji równoważnych Wykonawca zobowiązany jest do przeprowadzenia przeszkolenia zgodnie z wymogami z niniejszego Rozdziału.
 4. Wykonawca zobowiązuje się do instalacji i konfiguracji Oprogramowania równoważnego w terminie do 10 Dni Roboczych od dnia zawarcia Umowy.
 5. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie Oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest oferowanie Oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.
6. Wykonawca w ramach instalacji:
 - a) dokona czynności instalacji i konfiguracji oprogramowania równoważnego na Platformie Sprzętowo – Programowej Zamawiającego, o której mowa w pkt 3,
 - b) dokona czynności instalacji i konfiguracji agentów Oprogramowania na Platformie Sprzętowo - Programowej Zamawiającego w monitorowanym środowisku złożonym z 205 serwerów.
 - c) w przypadku, gdy zaoferowane Oprogramowanie nie będzie współdziałać

ze Środowiskiem Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy tego Środowiska, Wykonawca na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie tego Środowiska,

- d) w przypadku, gdy oferowane Oprogramowanie będzie wymagało dodatkowych licencji niezbędnych do jego uruchomienia na ww. systemach operacyjnych Wykonawca zobowiązany jest dostarczyć je na swój koszt,
- e) dokona wydzielenia usług i aplikacji działających w systemach objętych monitorowaniem oraz skonfiguruje oprogramowanie równoważne na potrzeby Zamawiającego (min. 10 pulpitów nawigacyjnych),
- f) przeprowadzi przeszkolenie zgodnie z poniższymi założeniami:
 - i. Wykonawca w przypadku dostarczenia Oprogramowania równoważnego zobowiązany jest do przeprowadzenia w formie zdalnej przeszkolenia dla pracowników Zamawiającego, które będzie obejmowało co najmniej zagadnienia z zakresu administrowania, konfiguracji oraz zarządzania zaoficerowanym Oprogramowaniem,
 - ii. Wykonawca najpóźniej w dniu podpisania Umowy przedstawi do zatwierdzenia Zamawiającemu zakres przeszkolenia, kwalifikacje Wykładowcy, materiały szkoleniowe, harmonogram przeszkolenia,
 - iii. Przeszkolenie odbędzie się w jednej turze dla maksymalnie 10 uczestników ze strony Zamawiającego. Przeszkolenie będzie trwać minimum 24 godziny, jednak nie więcej niż 8 godzin jednego dnia, dzień po dniu, w Dni Robocze,
 - iv. Wykonawca w ramach warsztatu zapewni salę szkoleniową na terenie m.st. Warszawy wraz z wyżywieniem w postaci jednego gorącego posiłku (obiad) i napojów w czasie przerw każdego dnia dla każdego uczestnika.