WA.263.36.2021.MW Warszawa, dnia 24 listopada 2021 r.

Wykonawcy ubiegający się
o udzielenie zamówienia

Dotyczy: **postępowania o udzielenie zamówienia publicznego (nr WA.263.36.2021.MW) na odnowienie/dostawę licencji na oprogramowanie antywirusowe na 220 stanowisk wraz ze wsparciem technicznym, w tym prawo do aktualizacji oprogramowania, na okres 36 miesięcy.**

Odpowiedzi na pytania, zmiana terminu składania i otwarcia ofert oraz terminu związania ofertą

Pytanie nr 1

Informujemy Zamawiającego, że po zapoznaniu się z treścią postępowania oznaczonego znakiem **2021/BZP 00274690/01** dla Centrum Projektów Europejskich, Domaniewska 39a Warszawa. Po analizie opisu przedmiotu zamówienia i kontakcie z producentami rozwiązań z obszaru bezpieczeństwa sieci działającymi w Polsce lub posiadającymi swoje centrum serwisowe w Polsce, oświadczamy, że sposób w jaki został opisany przedmiot zamówienia w rażący sposób narusza przepisy art. 7 ust. 1 PZP i art. 29 ust. 1, 2 i 3 PZP. Opis przedmiotu oprogramowania równoważnego został bezpośrednio skopiowany ze strony obecnego dostawcy, co automatycznie wyklucza innych dostawców oprogramowania antywirusowego. Żaden obecny dostawca nie jest w stanie spełnić wymogi dotyczące oprogramowania równoważnego, mimo iż działanie oprogramowania jest równoważne bądź lepsze.

Zwracam się z prośbą do Zamawiającego o dopuszczenie poniższych parametrów równoważności :

1. System scentralizowanego zarządzania powinien obsługiwać następujące systemy operacyjne:

   Microsoft Windows 11 Home 64-bitowy

   Microsoft Windows 11 Pro 64-bitowy

   Microsoft Windows 11 Enterprise 64-bitowy

   Microsoft Windows 11 Education 64-bitowy

   Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-bitowy/64-bitowy

   Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-bitowy/64-bitowy

   Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-bitowy/64-bitowy

   Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-bitowy/64-bitowy

   Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-bitowy/64-bitowy

   Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-bitowy/64-bitowy

   Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-bitowy/64-bitowy

   Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-bitowy/64-bitowy

   Microsoft Windows 10 20H2 32-bitowy/64-bitowy

Microsoft Windows 10 20H1 32-bitowy/64-bitowy

Microsoft Windows 10 Enterprise 2019 LTSC 32-bitowy/64-bitowy

Microsoft Windows 10 Enterprise 2016 LTSB 32-bitowy/64-bitowy

Microsoft Windows 10 Enterprise 2015 LTSB 32-bitowy/64-bitowy

Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-bitowy/64-bitowy

Microsoft Windows 10 Pro for Workstations RS5 (October 2018 Update, 1809) 32-bitowy/64-bitowy

Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-bitowy/64-bitowy

Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-bitowy/64-bitowy

Microsoft Windows 10 Pro 19H1 32-bitowy/64-bitowy

Microsoft Windows 10 Pro for Workstations 19H1 32-bitowy/64-bitowy

Microsoft Windows 10 Enterprise 19H1 32-bitowy/64-bitowy

Microsoft Windows 10 Education 19H1 32-bitowy/64-bitowy

Microsoft Windows 10 Home 19H2 32-bitowy/64-bitowy

Microsoft Windows 10 Pro 19H2 32-bitowy/64-bitowy

Microsoft Windows 10 Pro for Workstations 19H2 32-bitowy/64-bitowy

Microsoft Windows 10 Enterprise 19H2 32-bitowy/64-bitowy

Microsoft Windows 10 Education 19H2 32-bitowy/64-bitowy

Microsoft Windows 8.1 Pro 32-bitowy/64-bitowy

Microsoft Windows 8.1 Enterprise 32-bitowy/64-bitowy

Microsoft Windows 8 Pro 32-bitowy/64-bitowy

Microsoft Windows 8 Enterprise 32-bitowy/64-bitowy

Microsoft Windows 7 Professional z pakietem Service Pack 1 i nowszym 32-bitowy/64-bitowy

Microsoft Windows 7 Enterprise/Ultimate z pakietem Service Pack 1 i nowszym 32-bitowy/64-bitowy

Windows Server 2022 Standard 64-bitowy

Windows Server 2022 Core 64-bitowy

Windows Server 2022 Datacenter 64-bitowy

Windows Server 2019 Standard 64-bitowy

Windows Server 2019 Core 64-bitowy

Windows Server 2019 Datacenter 64-bitowy

Windows Server 2016 Standard (LTSB) 64-bitowy

Windows Server 2016 Server Core (Opcja instalacji) (LTSB) 64-bitowy

Windows Server 2016 Datacenter (LTSB) 64-bitowy

Windows Server 2012 R2 Standard 64-bitowy

Windows Server 2012 R2 Server Core 64-bitowy

Windows Server 2012 R2 Foundation 64-bitowy

Windows Server 2012 R2 Essentials 64-bitowy

Windows Server 2012 R2 Datacenter 64-bitowy

Windows Server 2012 Standard 64-bitowy

Windows Server 2012 Server Core 64-bitowy

Windows Server 2012 Foundation 64-bitowy

Windows Server 2012 Essentials 64-bitowy

Windows Server 2012 Datacenter 64-bitowy

Windows Server 2008 R2 Standard z pakietem Service Pack 1 i nowszy 64-bitowy

Windows Server 2008 R2 z pakietem Service Pack 1 (wszystkie wersje) 64-bitowy

Windows Storage Server 2016 64-bitowy

Windows Storage Server 2012 R2 64-bitowy

Windows Storage Server 2012 64-bitowy

2. System scentralizowanego zarządzania powinien przechowywać ustawienia w relacyjnej bazie danych:

Microsoft SQL Server 2012 Express 64-bitowy

Microsoft SQL Server 2014 Express 64-bitowy

Microsoft SQL Server 2016 Express 64-bitowy

Microsoft SQL Server 2017 Express 64-bitowy

Microsoft SQL Server 2019 Express 64-bitowy

Microsoft SQL Server 2014 (wszystkie wersje) 64-bitowy

Microsoft SQL Server 2016 (wszystkie wersje) 64-bitowy

Microsoft SQL Server 2017 (wszystkie wersje) na 64-bitowy system Windows

Microsoft SQL Server 2017 (wszystkie wersje) na 64-bitowy system Linux

Microsoft SQL Server 2019 (wszystkie edycje) na 64-bitowy system Windows (wymaga dodatkowych działań)

Microsoft SQL Server 2019 (wszystkie edycje) na 64-bitowy system Linux (wymaga dodatkowych działań)

MySQL 5.7 Community 32-bitowy/64-bitowy

MySQL Standard Edition 8.0 32-bitowy/64-bitowy

MySQL Enterprise Edition 8.0 32-bitowy/64-bitowy

Wszystkie obsługiwane wersje serwera SQL w platformach chmury Amazon RDS i Microsoft Azure

MariaDB Server 10.3 32-bitowy/64-bitowy z silnikiem magazynowania InnoDB

MariaDB Galera Cluster 10.3 32-bitowy/64-bitowy z silnikiem magazynowania InnoDB

3. System zdalnego zarządzania powinien posiadać polskojęzyczny interfejs konsoli programu.
4. System zdalnego zarządzania powinien umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych odpowiadających strukturze sieci (grupy robocze sieci Microsoft Windows i/lub struktura Active Directory).
5. System zdalnego zarządzania powinien umożliwiać automatyczne umieszczanie stacji roboczych w określonych grupach administracyjnych w oparciu o zdefiniowane reguły.
6. System zdalnego zarządzania powinien posiadać jeden pakiet instalacyjny dla stacji roboczej jak również systemów serwerowych.
7. System zdalnego zarządzania powinien umożliwiać ograniczenie pasma sieciowego wykorzystywanego do komunikacji stacji z serwerem administracyjnych. Reguły powinny umożliwić ograniczenia w oparciu o zakresy adresów IP oraz przedziały czasowe.
8. System zdalnego zarządzania umożliwia tworzenie hierarchicznej struktury serwerów administracyjnych jak również tworzenie wirtualnych serwerów administracyjnych.
9. System zdalnego zarządzania umożliwia zarządzanie stacjami roboczymi i serwerami plików Windows, nawet wtedy, gdy znajdują się one za zaporą NAT/Firewall.
10. Komunikacja pomiędzy serwerem zarządzającym a agentami sieciowymi na stacjach roboczych jest szyfrowana przy użyciu protokołu SSL.
11. Konsola administracyjna posiada możliwość zdalnego inicjowania skanowania antywirusowego na stacjach roboczych włączonych do sieci komputerowych w całej firmie.
12. Zarządzanie aplikacjami odbywa się przy użyciu profili aplikacji oraz zadań.
13. Konsola administracyjna ma możliwość informowania administratorów o wykryciu epidemii wirusa.
14. Serwer zarządzający ma możliwość automatycznej reakcji na epidemie wirusa (automatyczne stosowanie wskazanego profilu ustawień stacji roboczych oraz uruchomienia odpowiednich zadań).
15. System centralnego zarządzania wyposażony w mechanizmy raportowania i dystrybucji oprogramowania oraz polityk antywirusowych w sieciach korporacyjnych.
16. System centralnej dystrybucji i instalacji aktualizacji bibliotek sygnatur wirusów, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji biblioteki.
17. System centralnej dystrybucji i instalacji aktualizacji oprogramowania, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowego

oprogramowania.

18. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.
19. System centralnego zarządzania powinien zapewniać obsługę trybu dynamicznego dla Virtual Desktop Infrastructure (VDI).
20. System centralnego zbierania informacji i tworzenia sumarycznych raportów.
21. System zdalnego zarządzania powinien umożliwiać automatyczne wysyłanie raportów pocztą elektroniczną lub zapisywanie ich w postaci plików w zdefiniowanej lokalizacji (przynajmniej w formatach HTML, XML i PDF).
22. System zdalnego zarządzania powinien umożliwiać podgląd w czasie rzeczywistym statystyk ochrony, stanu aktualizacji instalacji w sieci itp.
23. System zdalnego zarządzania powinien umożliwiać tworzenie kategorii aplikacji i warunków ich uruchomienia.
24. System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o aplikacjach i plikach wykonywalnych znajdujących się na stacjach roboczych.
25. Program powinien mieć możliwość dezinstalacji aplikacji niekompatybilnych jak również dowolnej aplikacji znajdującej się w rejestrze aplikacji użytkownika.
26. System zdalnego zarządzania powinien wyświetlać szczegółowe informacje na temat luk w oprogramowaniu wykrytych na zarządzanych komputerach
27. System zdalnego zarządzania powinien mieć możliwość zbierania informacji o sprzęcie zainstalowanym na komputerach klienckich.
28. System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o obiektach poddanych kwarantannie oraz podejmowanie odpowiednich działań (np. przywracanie, skanowanie itp.).
29. System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o kopiach zapasowych obiektów wyleczonych/usuniętych na stacjach roboczych wraz z możliwością ich przywrócenia do początkowej lokalizacji i/lub zapisania na stacji administratora.
30. System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o obiektach, które zostały wykryte ale program nie podjął względem nich żadnego działania wraz z możliwością wymuszenia przez administratora odpowiedniego działania.
31. System zdalnego zarządzania powinien umożliwiać automatyczne instalowanie licencji na stacjach roboczych.
32. System zdalnego zarządzania powinien umożliwiać automatyczne i regularne tworzenie kopii zapasowej serwera zarządzającego, która umożliwi przywrócenie w pełni działającego systemu zarządzania.
33. System zdalnego zarządzania powinien umożliwiać automatyczne uruchomienie wyłączonych komputerów przed wykonaniem odpowiednich zadań administracyjnych (z wykorzystaniem funkcji Wake-On-LAN) a po zakończeniu wykonywania zadań ich wyłączenie. Funkcjonalność

ta nie może być ograniczona tylko do podsieci, w której znajduje się serwer administracyjny.

34. System zdalnego zarządzania powinien umożliwiać wysłanie do stacji roboczych komunikatu o dowolnie zdefiniowanej treści.
35. System zdalnego zarządzania powinien umożliwiać zdalne włączanie, wyłączanie oraz restartowanie komputerów wraz z możliwością interakcji z użytkownikiem (np. natychmiastowe wykonanie działania lub jego odłożenie na zdefiniowany okres czasu).
36. Program powinien umożliwiać ukrycie przed użytkownikiem interfejsu aplikacji, ikony w pasku systemowym, wpisów w Menu Start oraz na liście zainstalowanych programów.
37. Program powinien umożliwić administratorowi wyłączenie niektórych lub wszystkich powiadomień wyświetlanych na stacjach roboczych.
38. System zdalnego zarządzania powinien umożliwiać administrację poprzez przeglądarkę internetową.
39. System zdalnego zarządzania powinien dać możliwość wykorzystania bramy połączenia dla komputerów, które nie mają bezpośredniego połączenia z Serwerem administracyjnym.
40. System zdalnego zarządzania powinien mieć możliwość sprawdzenia aktualnych wersji oprogramowania antywirusowego.
41. System zdalnego zarządzania powinien tworzyć listę kont użytkowników sieci. Do tworzenia powinny być wykorzystywane różne źródła w tym min. AD, kontrolery domen oraz lokalne konta na komputerach.
42. System zdalnego zarządzania powinien umożliwić wysyłanie powiadomień do wybranych użytkowników przy użyciu poczty elektronicznej lub wiadomości SMS.
43. System zdalnego zarządzania powinien umożliwić instalowanie certyfikatów na urządzeniach mobilnych wybranych użytkowników.
44. System zdalnego zarządzania powinien umożliwić instalowanie certyfikatów iOS MDM na urządzeniach mobilnych wybranych użytkowników.
45. System zdalnego zarządzania powinien tworzyć repozytorium sprzętu w tym min. komputerów i nośników wymiennych.
46. Administrator powinien mieć możliwość dopisywania informacji do sprzętu w repozytorium w tym min. numeru ewidencyjnego, numeru seryjnego, producenta, daty zakupu, aktualnego użytkownika.
47. Administrator powinien mieć możliwość zaznaczenia czy urządzenie jest lub nie jest aktualnie wykorzystywane.
48. Administrator powinien mieć możliwość oznaczania urządzeń jako firmowe.
49. System zdalnego zarządzania powinien umożliwić zarządzanie urządzeniami mobilnymi z wykorzystaniem serwerów Exchange ActiveSync i iOS MDM.
50. Zarządzanie urządzeniami przenośnymi Exchange ActiveSync powinno umożliwiać przypisywanie ustawień do wybranych kont pocztowych. Ustawienia powinny obejmować w zależności od systemu operacyjnego przynajmniej synchronizacje poczty, korzystanie z

określonych aplikacji, ustawienie hasła użytkownika, szyfrowanie danych.

51. Zarządzanie urządzeniami przenośnymi iOS MDM powinno umożliwiać przynajmniej dodawanie i zmienianie profili konfiguracji, instalować profile zabezpieczeń, instalować aplikacje na urządzeniu przenośnym, zablokować urządzenie przenośne, zresetować hasło urządzenia lub usunąć z niego wszystkie dane.
52. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
53. W całym okresie trwania subskrypcji użytkownik ma możliwość pobierania i instalacji nowszych wersji oprogramowania i konsoli zarządzającej.

Odpowiedź 1

Zamawiający dokonał zmiany brzmienia opisu przedmiotu zamówienia, który otrzymał nowe brzmienie, tj. :
„ Obecnie Centrum Projektów Europejskich posiada oprogramowanie antywirusowe ESET Endpoint Antyvirus Suite, który według producenta zmienił nazwę na ESET PROTECT Essential ON-PREM.
Przedmiotem zamówienia jest **odnowienie licencji na 220 urządzeń na oprogramowanie antywirusowe ESET na okres 36 miesięcy**. Identyfikator aktualnej licencji EAV-0220434057.
Optymalnym rozwiązaniem byłoby przedłużenie posiadanej licencji, jednak Zamawiający dopuszcza możliwość zaoferowania produktów równoważnych w zakresie nowej licencji na oprogramowanie antywirusowe (oprogramowanie równoważne). Przy zmianie oprogramowania musi być zapewnione wsparcie w zakresie migracji, instalacji (w siedzibie Zamawiającego w Warszawie, ul. Domaniewska 39a oraz w Krakowie, Gdańsku, Wrocławiu i Olsztynie) przez Wykonawcę lub Producenta oprogramowania na czas zaplanowanego wdrożenia przez Zamawiającego na wszystkich wymaganych urządzeniach (około 220 urządzeń). Koszt migracji, instalacji i wdrożenia nowego oprogramowania musi być wliczony w cenę licencji. Migracja i instalacja zmienionego oprogramowania musi zostać wykonana w terminie 7 dni od dnia dostawy oprogramowania.

Zamawiający dopuszcza produkt równoważny, którego funkcjonalność pokrywa się z funkcjami ESET PROTECT Essential ON-PREM. W przypadku rozwiązania równoważnego Zamawiający wymaga przeprowadzenia przez wykonawcę migracji, instalacji i wdrożenia oprogramowania (instalacja na wszystkich stanowiskach wskazanych przez Zamawiającego) oraz przeprowadzenie szkolenia informatyków (2 osoby) w zakresie obsługi oprogramowania.

Równoważność oznacza, że:

a. oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem (Windows 7, 8, 10, Windows Server 2008, 2008 R2, 2012, 2012 R2, 2019, 32-bit oraz 64-bit) i sprzętem funkcjonującym u Zamawiającego;

b. oprogramowanie równoważne musi zapewniać co najmniej pełną funkcjonalność oprogramowania w stosunku, do którego jest wskazywana przez wykonawcę jako równoważne i posiadać co najmniej takie same parametry techniczne i funkcjonalne;

c. warunki licencji oprogramowania równoważnego w każdym aspekcie licencjonowania muszą być nie gorsze niż licencje oprogramowania wskazanego przez Zamawiającego w stosunku do którego jest równoważna;

d. warunki i zakres licencji dla oprogramowania równoważnego muszą być nie gorsze niż dla oprogramowania wskazanego przez Zamawiającego w stosunku do którego jest równoważna.

3. Zamawiający wymaga, aby wykonawca w formularzu ofertowym opisał wszystkie dane techniczne składające się na dany asortyment zgodnym z zamówieniem.

Uwaga:
1) W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne".
2) W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne".
4) Wykonawca, który powoła się na oprogramowanie równoważne w zakresie opisanym przez Zamawiającego, jest obowiązany wykazać w ofercie, że oferowany przez niego przedmiot dostawy spełnia wymagania określone przez Zamawiającego.
5) Ciężar dowodowy w zakresie udowodnienia równoważności zaoferowanego oprogramowania z opisanymi warunkami równoważności spoczywa na Wykonawcy, składającym ofertę równoważną.
6) Zamawiający wymaga, aby zaoferowane przez Wykonawcę oprogramowanie równoważne nie powodowało konieczności wykonania dodatkowych prac integracyjnych po stronie Zamawiającego, tym samym poniesienia dodatkowych, niezaplanowanych kosztów.
7) W celu potwierdzenia, iż oferowana dostawa spełnia wymagania określone przez Zamawiającego, Wykonawca, który zaoferuje oprogramowanie równoważne do wskazanego przez Zamawiającego załączy do oferty szczegółową specyfikację techniczną dla oferowanego oprogramowania równoważnego, wystawioną przez producenta oferowanego oprogramowania równoważnego, zawierającą opis wszystkich cech i funkcjonalności oferowanego oprogramowania równoważnego.
8) Oprogramowanie musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego oprogramowania nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.

Obecnie użytkowane przez Zamawiającego oprogramowanie antywirusowe zapewnia poniższe funkcje (….). „

Zał. nr 2 stanowi zał. nr 1 do niniejszego pisma.

Zamawiający przedłuża termin składania ofert do dnia 29 listopada 2021 roku i dokonuje poniższych zmian w SWZ:

1. W rozdziale XI pkt 1 otrzymuje brzmienie:

*„1. Wykonawca jest związany ofertą od dnia upływu terminu składania ofert przez 30 (trzydzieści) dni kalendarzowych tj. do dnia **28.12.2021 r.”***;

2. W rozdziale XIII pkt 2 otrzymuje brzmienie:

*„2. Ofertę wraz z wymaganymi załącznikami należy złożyć w terminie do dnia **29.11.2021 r**., do godz. **10.00.”***;

3. W rozdziale XIV pkt 1 otrzymuje brzmienie:

*„1. Otwarcie ofert nastąpi w dniu **29.11.2021 r**. o godzinie **11.00.”***

ZATWIERDZAM

Mirosław Marczewski

Elektronicznie podpisany przez Mirosław Marczewski
Data: 2021.11.24 13:14:58 +01'00'