AG/ZP-16/2022 Załącznik nr 3b do SWZ

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – ZESTAWIENIE WYMAGANYCH PARAMETRÓW TECHNICZNYCH**

**Oprogramowanie antywirusowe**

Zamawiający aktualnie posiada:

* ESET Security Management Center (Server), Wersja 7.2 (7.2.1266.0)
* ESET Security Management Center (Konsola internetowa), Wersja 7.2 (7.2.221.0)
* licencje klienckie: ESET Endpoint Antivirus + ESET Server Security (ESET File Security): 170 sztuk ważne do 19.07.2023

|  |  |  |  |
| --- | --- | --- | --- |
| **lp**. | **Parametry techniczne – warunki graniczne** | **Parametr wymagany**  | **Parametr oferowany**  |
|  |  |  |  |
|  | **Oprogramowanie antywirusowe** |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| AVP-001 | Przedmiot zamówienia obejmuje dostawę 30 licencji klienckich wspieranych przez posiadany serwer oprogramowania antywirusowego na okres 36 miesięcy. | Tak |  |

**Rozwiązanie równoważne - wymagania minimalne**

W przypadku dostawy innego rozwiązania Wykonawca musi dostarczyć oprogramowanie antywirusowe na min 200 licencji na okres 36 miesięcy spełniające wskazane wymagania minimalne:

|  |  |  |  |
| --- | --- | --- | --- |
| **lp**. | **Parametry techniczne – warunki graniczne** | **Parametr wymagany**  | **\*Parametr oferowany**  |
|  |  |  |  |
|  | **Oprogramowanie antywirusowe** |  |  |
| 1 | Oprogramowanie musi umożliwiać automatyczną (zdalną) instalację na stacjach klienckich, bez dostępu do Internetu. | Tak |  |
| 2 | Oprogramowanie musi umożliwiać automatyczną dystrybucję bazy sygnatur wirusów i aktualizacji komponentów programu w sieci wydzielonej, bez dostępu do Internetu (funkcjonalność serwera kopii dystrybucyjnej). | Tak |  |
| 3 | Oprogramowanie musi posiadać wbudowane narzędzie do analizy i gromadzenia wszystkich ważnych informacji o danym komputerze, bez konieczności korzystania z żadnych zewnętrznych stron internetowych, w szczególności o następujących funkcjonalnościach:1. możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach;
2. konsola zarządzająca zapewniająca automatyczną synchronizację z Active Directory;
3. możliwość automatycznego wykrywania i usuwania innego oprogramowania antywirusowego podczas instalacji;
4. możliwość ukrycia interfejsu przed użytkownikiem końcowym;
5. posiadać kwarantannę dla programów szpiegujących (spyware oraz riskware);
6. możliwość stworzenia pliku diagnostycznego do analizy problemów;
7. posiadać narzędzie ręcznej aktualizacji stacji roboczych we wszystkich sygnaturach dla poszczególnych silników skanujących;

automatyczne powiadamianie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem, czy stacja robocza jest odpowiednio zabezpieczona.  | Tak |  |
| 4 | Oprogramowanie musi posiadać wbudowany moduł heurystyczny. | Tak |  |
| 5 | Oprogramowanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. | Tak |  |
| 6 | Oprogramowanie musi być wyposażone w system zapobiegania włamaniom działający na hoście zapewniający pracę z regułami, gdzie aplikacja automatycznie tworzy i wykorzystuje reguły. Tworzenie reguł musi odbywać się co najmniej w oparciu o:1. aplikacje źródłowe;
2. pliki docelowe;
3. aplikacje docelowe;

elementy docelowe rejestru systemowego. | Tak |  |
| 7 | Oprogramowanie musi umożliwiać całkowitą, niekolidującą z pracą systemu operacyjnego i automatyczną, deinstalację oprogramowania na stacji klienckiej. | Tak |  |
| 8 | Do instalacji serwera centralnej administracji nie może być wymagane zainstalowanie żadnych dodatkowych płatnych silników baz danych. Serwer centralnej administracji musi mieć własną wbudowaną bazę. | Tak |  |
| 9 | Wykonawca musi dostarczyć licencję na system operacyjny umożliwiający zainstalowanie i korzystanie z serwera centralnej administracji. | Tak |  |
| 10 | Serwer centralnej administracji musi oferować administratorowi możliwość współpracy przynajmniej z jednym z wymienionych zewnętrznych silników baz danych: Microsoft SQL Server, MySQL Server. | Tak |  |
| 11 | Oprogramowanie musi umożliwiać instalację i poprawne funkcjonowanie klienta AV na następujących systemach operacyjnych: Windows 7 i nowsze, Windows Server 2012 i nowsze, Linux. | Tak |  |
| 12 | Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów. | Tak |  |
| 13 | Wraz z dostawą oprogramowania z licencjami Wykonawca zobowiązuje się do:1. dostarczenia instrukcji konfiguracji serwera aktualizacji w ramach zasobów Zamawiającego;
2. dostarczenia instrukcji instalacji Oprogramowania na serwerze aktualizacji;
3. dostarczenia instrukcji konfiguracji Oprogramowania;
4. dostarczenia instrukcji generowania pakietów instalacyjnych na stacje robocze użytkowników końcowych;
5. dostarczenia dokumentacji eksploatacyjnej obejmującej instrukcje związane z administracją i eksploatacją rozwiązania, procedury awaryjne i testowe;
6. dostarczenia instrukcji instalacji pakietów na stacjach roboczych przez użytkowników;

przeszkolenia dwóch administratorów. | Tak |  |
| 14 | Szkolenie dla administratorów dotyczące oferowanego oprogramowania musi spełniać następujące wymagania:1. być przeprowadzone przez certyfikowanego trenera oferowanego oprogramowania;
2. obejmować zakresem:
	1. konfigurowanie i administrowanie od strony klienta;
	2. konfigurowanie i administrowanie od strony konsoli zarządzającej oprogramowaniem;

odbyć się online w terminie uzgodnionym z Zamawiającym jednak nie później niż w ciągu 5 dni roboczych od dostawy oprogramowania z licencjami. | Tak |  |
| 15 | Oprogramowanie nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie z art. 4 pkt. 7 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz. U. z 2020 r. poz. 1369 z późn. zm.), dalej: „Ustawa”, należy do Krajowego systemu cyberbezpieczeństwa, którego celem jest zgodnie z art. 3 Ustawy, zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. W związku z tym, oprogramowanie musi być zgodne z celem Krajowego systemu cyberbezpieczeństwa i przepisami Ustawy oraz nie może zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa. | Tak |  |
| 16 | Dostarczana licencja oprogramowania musi pochodzić z autoryzowanego przez producenta kanału dystrybucji. Wykonawca jest zobowiązany dostarczyć Zamawiającemu dowody poświadczające autentyczność zakupionych licencji na zasadach określonych przez producenta wraz z dostawą oprogramowania. | Tak |  |

\* wypełnia Wykonawca

UWAGA!!!

**Brak wpisu w polach parametr oferowany lub nie spełnienie zapisów poszczególnych warunków parametrów wymaganych spowoduje odrzucenie oferty Wykonawcy.**

Oświadczamy, że oferowane urządzenie/sprzęt/wyposażenie jest kompletne i będzie po zainstalowaniu gotowe do pracy bez żadnych dodatkowych zakupów.

.................................................................................

 miejscowość i data

 ...............................................................................

 podpis i pieczątka osoby uprawnionej