**Załącznik nr 1 do SWZ**

**Opis przedmiotu zamówienia**

**(zwany dalej: „OPZ”)**

**w postępowaniu nr ZP/7/2024/JK**

**pn.: „Przedłużenie subskrypcji dla posiadanych przez Zamawiającego licencji oprogramowania antywirusowego**”

48000000-8 Pakiety oprogramowania i systemy informatyczne

48761000-0 Pakiety oprogramowania antywirusowego

1. Zamawiający - Centrum Projektów Polska Cyfrowa (dalej: „CPPC”), jest obecnie uprawnionym posiadaczem klucza licencyjnego programu antywirusowego „ESET PROTECT Entry ON-PREM” (Identyfikator publiczny licencji: 333-4E3-3DR), tj. ESET Endpoint Security + ESET Server Security dla urządzeń **z terminem ważności do dnia 23 maja 2024 roku.**
2. Przedmiotem zamówienia jest:
3. dostawa zbiorowego prawa do aktualizacji (subskrypcji) oprogramowania antywirusowego „ESET PROTECT Entry ON-PREM”, tj. ESET Endpoint Security + ESET Server Security lub rozwiązania równoważnego, na okres 36 miesięcy dla 300 (słownie: trzystu) stacji roboczych, serwerów i urządzeń mobilnych;
4. dostawa dokumentów potwierdzających autentyczność i legalność oferowanego oprogramowania, łącznie ze wszystkimi składnikami niezbędnymi do potwierdzenia legalności ich pochodzenia, np.: oryginalny nośnik, certyfikat autentyczności, kod aktywacyjny wraz z instrukcją aktywacji, jeśli jest to niezbędne dla nabycia przez Zamawiającego praw do tego oprogramowania lub jego uruchomienia,
5. **Wykonawca zobowiązany jest do dostarczenia składników, o których mowa w lit. a i b, w maksymalnym terminie do 3 dni kalendarzowych od dnia podpisania Umowy,** na własny koszt i ryzyko, do siedziby Zamawiającego, mieszczącej się przy ul. Spokojnej 13a, 01-044 Warszawa;
6. świadczenie w okresie, o którym mowa w lit. a bezpłatnych konsultacji telefonicznych (Zamawiający dopuszcza wsparcie w ramach hotline producenta) w języku polskim w zakresie wsparcia technicznego producenta oprogramowania i dostępu do aktualizacji baz wirusów w okresie ważności licencji. Konsultacje powinny być możliwe co najmniej w dni robocze, w godzinach 8:00-16:00,
7. zapewnienie nieodpłatnego korzystania z uaktualnień baz sygnatur wirusów przez okres 36 miesięcy od dnia uruchomienia subskrypcji.
8. prawo do pobierania nieodpłatnie nowszych wersji oprogramowania w ramach dostarczonych licencji przez okres 36 miesięcy od dnia uruchomienia subskrypcji.
9. W przypadku stwierdzenia przez Zamawiającego niezgodności dostarczonego asortymentu z Opisem przedmiotu zamówienia, wykonawca wymieni go na produkt wolny od wad, spełniający wymagania Zamawiającego, w terminie do 3 dni roboczych od dnia zgłoszenia informacji przez Zamawiającego. Zgłoszenie nastąpi za pośrednictwem poczty elektronicznej, na adres e-mail wskazany w umowie.
10. Zamawiający dopuszcza zastosowanie innego równoważnego rozwiązania-systemu antywirusowego (zwanego też: „Programem”) wraz z kontrolą dostępu do stron internetowych, dwukierunkowym firewallem i filtrem antyspamowym centralnie zarządzanym, pod warunkiem dostarczenia nowych licencji nowego oprogramowania, w liczbie wskazanej w ust. 2 lit. a, spełniającego łącznie poniższe minimalne wymagania funkcjonalne dla rozwiązania równoważnego:

|  |  |
| --- | --- |
| **Opis wymagań minimalnych – opis kryteriów równoważności** | |
| **Wymagania ogólne** | |
| AV-01 | Program musi wspierać platformę Microsoft Windows 10 Pro x86 / х64 i nowsze |
| AV-02 | Program musi posiadać polskojęzyczny interfejs konsoli programu i jego monitora na stacjach roboczych. |
| AV-03 | Program musi posiadać certyfikat AV-Comparatives lub AV-TEST lub równoważny certyfikat niezależnych laboratoriów |
| AV-04 | Program musi zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami i innymi potencjalnie niebezpiecznymi programami. |
| AV-05 | Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów. |
| AV-06 | Program musi posiadać możliwość wyeksportowania bieżącej konfiguracji programu w celu jej późniejszego zaimportowania na tym samym lub innym komputerze. |
| AV-07 | Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju. |
| AV-08 | Dostarczane licencje muszą być bezterminowe, tj. po wygaśnięciu subskrypcji musi istnieć możliwość dalszego korzystania z oprogramowania, bez żadnych zakłóceń w działaniu komputera, na którym jest zainstalowane, z ostatnią możliwą datą aktualizacji szczepionek. |
| AV-09 | Program musi posiadać możliwość aktualizacji zarówno samego oprogramowania, jak i bazy sygnatur, szczepionek itp. przez okres co najmniej 36 miesięcy od dnia obioru przedmiotu umowy. |
| **Ochrona w czasie rzeczywistym** | |
| AV-10 | Program musi posiadać możliwość skanowania i klasyfikowania plików oraz odsyłaczy do zasobów sieciowych na podstawie informacji gromadzonych w oparciu o technologię chmury. |
| AV-11 | Program musi posiadać dedykowany moduł blokujący określone kategorie urządzeń (np. pamięci masowe, urządzenia Bluetooth, itp.), w tym:   * Możliwość tworzenia reguł blokujących/zezwalających na korzystanie z danego urządzenia w zależności od konta, na którym pracuje użytkownik. * Możliwość utworzenia listy zaufanych urządzeń na podstawie modelu, bądź identyfikatora urządzenia dla określonego konta użytkownika systemu Windows. |
| AV-12 | Ochrona przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem. |
| AV-13 | Możliwość wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich. |
| AV-14 | Wbudowany moduł skanujący ruch HTTP w czasie rzeczywistym niezależnie od przeglądarki. |
| AV-15 | Wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa. |
| AV-16 | Możliwość określenia poziomu czułości modułu heurystycznego. |
| AV-17 | Wbudowany moduł kontrolujący dostęp do rejestru systemowego. |
| AV-18 | Moduł zapory ogniowej z możliwością zdefiniowania zaufanych podsieci, dla których nie będą stosowane żadne reguły zapory. |
| AV-19 | Ochrona przed niebezpiecznymi rodzajami aktywności sieciowej i atakami; możliwość tworzenia reguł wykluczających dla określonych adresów/zakresów IP. |
| AV-20 | Centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym. |
| AV-21 | Leczenie i usuwanie plików z archiwów co najmniej następujących formatów: RAR, ARJ, ZIP, CAB, JAR. |
| AV-22 | Możliwość zablokowania dostępu do ustawień programu dla użytkowników nie posiadających uprawnień administracyjnych. |
| AV-23 | Terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur. |
| AV-24 | Możliwość kontroli nad funkcjonalnością (włączenie / wyłączenie) wysłania podejrzanego obiektu do producenta oprogramowania antywirusowego w celu analizy, bezpośrednio z programu - do tego celu nie może być wykorzystany klient pocztowy |
| AV-25 | Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego. |
| AV-26 | Program musi posiadać funkcję chroniącą pliki, foldery i klucze rejestru wykorzystywane przez program przed zapisem i modyfikacją. |
| AV-27 | Program musi posiadać możliwość wyłączenia zewnętrznej kontroli usługi antywirusowej. |
| AV-28 | Program musi posiadać możliwość zablokowania operacji zamykania programu, zatrzymywania zadań, wyłączania ochrony, zmiany ustawień, usunięcia licencji oraz odinstalowania programu przy użyciu zdefiniowanej nazwy użytkownika i/lub hasła. |
| AV-29 | Program musi zapewnić autoryzację urządzeń podłączanych do portu USB. |
| **Skanowanie na żądanie** | |
| AV-30 | Skanowanie na żądanie uruchamianych, otwieranych, kopiowanych, przenoszonych lub tworzonych plików |
| AV-31 | W przypadku wykrycia wirusa monitor antywirusowy powinien automatycznie:   * Podejmować zalecane działanie, czyli próbować leczyć, a jeżeli nie jest to możliwe - usuwać obiekt; * Rejestrować w pliku raportu informację o wykryciu wirusa; * Powiadamiać administratora przy użyciu poczty elektronicznej lub poleceniem NET SEND; * Poddać kwarantannie podejrzany obiekt. |
| AV-32 | Skaner antywirusowy może być uruchamiany automatycznie zgodnie z terminarzem; skanowane są wszystkie lokalne dyski twarde komputera. |
| AV-33 | Informowanie o wykryciu podejrzanych działań uruchamianych aplikacji (np. modyfikacje rejestru, wtargnięcie do innych procesów) wraz z możliwością zezwolenia lub zablokowania takiego działania. |
| AV-34 | System antywirusowy musi posiadać możliwość skanowania archiwów i plików spakowanych, niezależnie od poziomu ich zagnieżdżenia. |
| **Aktualizacja baz danych sygnatur zagrożeń** | |
| AV-35 | Program musi posiadać możliwość określenia harmonogramu pobierania uaktualnień, w tym możliwość wyłączenia aktualizacji automatycznej. |
| AV-36 | Program musi posiadać możliwość pobierania uaktualnień modułów dla zainstalowanej wersji aplikacji. |
| AV-37 | Program musi posiadać możliwość określenia źródła uaktualnień. |
| AV-38 | Program musi posiadać możliwość skanowania obiektów poddanych kwarantannie po zakończonej aktualizacji. |
| AV-39 | Program musi posiadać możliwość cofnięcia ostatniej aktualizacji w przypadku uszkodzenia zestawu uaktualnień. |
| AV-40 | Program musi posiadać możliwość określenia ustawień serwera proxy w przypadku, gdy jest on wymagany do nawiązania połączenia z Internetem. |
| AV-41 | Antywirusowe bazy danych na serwerach producenta muszą być aktualizowane nie rzadziej niż raz na 4 godziny. |
| AV-42 | Pobieranie uaktualnień w trybie przyrostowym (np. po zerwaniu połączenia, bez konieczności retransmitowania już wczytanych fragmentów informacji). |
| **Raportowanie** | |
| AV-43 | Program musi posiadać możliwość raportowania zdarzeń informacyjnych. |
| **System Scentralizowanego Zarządzania** | |
| AV-44 | Dostarczone rozwiązanie antywirusowe musi posiadać system scentralizowanego zarządzania. Jeżeli do uruchomienia tego systemu konieczna jest odrębna licencja, należy ją dostarczyć wraz z oferowanym oprogramowaniem. |
| AV-45 | System Scentralizowanego Zarządzania musi wspierać co najmniej następujące platformy:   1. Microsoft Windows Server 2012 R2 Datacenter 64-bitowy lub nowszy 2. Microsoft Windows Server 2012 R2 Standard 64-bitowy lub nowszy |
| AV-46 | System scentralizowanego zarządzania musi przechowywać ustawienia w relacyjnej bazie danych Microsoft SQL Server lub innej dostarczanej wraz z rozwiązaniem. |
| AV-47 | System scentralizowanego zarządzania musi posiadać polskojęzyczny interfejs konsoli programu. |
| AV-48 | System scentralizowanego zarządzania musi umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych odpowiadających strukturze sieci (grupy robocze sieci Microsoft Windows i/lub struktura Active Directory). |
| AV-49 | System scentralizowanego zarządzania musi umożliwiać automatyczne umieszczanie stacji roboczych w określonych grupach administracyjnych w oparciu o zdefiniowane reguły. |
| AV-50 | System scentralizowanego zarządzania musi posiadać pakiet instalacyjny dla stacji roboczej, jak również systemów serwerowych. |
| AV-51 | System scentralizowanego zarządzania musi umożliwiać ograniczenie pasma sieciowego wykorzystywanego do komunikacji stacji z serwerem administracyjnym. Reguły powinny umożliwić ograniczenia w oparciu o zakresy adresów IP. |
| AV-52 | System scentralizowanego zarządzania umożliwia tworzenie hierarchicznej struktury serwerów administracyjnych, jak również tworzenie wirtualnych serwerów administracyjnych. |
| AV-53 | System scentralizowanego zarządzania umożliwia zarządzanie stacjami roboczymi i serwerami plików Windows nawet wtedy, gdy znajdują się one za zaporą NAT/Firewall. |
| AV-54 | Komunikacja pomiędzy serwerem zarządzającym a agentami sieciowymi na stacjach roboczych jest szyfrowana przy użyciu protokołu SSL. |
| AV-55 | Konsola administracyjna musi posiadać możliwość scentralizowanego inicjowania skanowania antywirusowego na stacjach roboczych włączonych do sieci komputerowej. |
| AV-56 | Zarządzanie aplikacjami odbywa się przy użyciu profili aplikacji oraz zadań. |
| AV-57 | Konsola administracyjna ma możliwość informowania administratorów o wykryciu epidemii wirusa. |
| AV-58 | Serwer zarządzający ma możliwość automatycznej reakcji na epidemie wirusa (automatyczne stosowanie wskazanego profilu ustawień stacji roboczych oraz uruchomienia odpowiednich zadań). |
| AV-59 | System centralnego zarządzania musi być wyposażony w mechanizmy raportowania i dystrybucji polityk antywirusowych w sieciach korporacyjnych. |
| AV-60 | System umożliwia centralną dystrybucję i instalację aktualizacji bibliotek sygnatur wirusów oraz umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji biblioteki. |
| AV-61 | System umożliwia centralną dystrybucję i instalację aktualizacji oprogramowania, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowego oprogramowania. |
| AV-62 | System scentralizowanego zarządzania musi umożliwiać automatyczne wysyłanie raportów pocztą elektroniczną lub zapisywanie ich w postaci plików w zdefiniowanej lokalizacji (przynajmniej w formacie PDF). |
| AV-63 | System scentralizowanego zarządzania musi umożliwiać podgląd w czasie rzeczywistym statystyk ochrony, stanu aktualizacji instalacji w sieci itp. |
| AV-64 | System scentralizowanego zarządzania musi umożliwiać przeglądanie informacji o aplikacjach znajdujących się na stacjach roboczych. |
| AV-65 | Program musi mieć możliwość dezinstalacji aplikacji niekompatybilnych, jak również dowolnej aplikacji znajdującej się w rejestrze aplikacji użytkownika. |
| AV-66 | System scentralizowanego zarządzania musi mieć możliwość zbierania informacji o sprzęcie zainstalowanym na komputerach klienckich. |
| AV-67 | System scentralizowanego zarządzania musi umożliwiać przeglądanie informacji o obiektach poddanych kwarantannie oraz musi umożliwiać podejmowanie odpowiednich działań (np. przywracanie, skanowanie itp.). |
| AV-68 | System scentralizowanego zarządzania musi umożliwiać przeglądanie informacji o obiektach, które zostały wykryte, ale program nie podjął względem nich żadnego działania. |
| AV-69 | System scentralizowanego zarządzania musi umożliwiać automatyczne instalowanie licencji dostarczonego oprogramowania antywirusowego na stacjach roboczych. |
| AV-70 | System scentralizowanego zarządzania musi umożliwiać automatyczne i regularne tworzenie kopii zapasowej serwera zarządzającego, która umożliwi przywrócenie w pełni działającego systemu zarządzania. |
| AV-71 | Program musi umożliwiać ukrycie przed użytkownikiem interfejsu aplikacji. |
| AV-72 | Program musi umożliwić administratorowi wyłączenie niektórych lub wszystkich powiadomień wyświetlanych na stacjach roboczych. |
| AV-73 | System scentralizowanego zarządzania musi umożliwiać administrację poprzez przeglądarkę internetową. |
| AV-74 | System scentralizowanego zarządzania musi dać możliwość wykorzystania bramy połączenia dla komputerów, które nie mają bezpośredniego połączenia z Serwerem administracyjnym. |
| AV-75 | System scentralizowanego zarządzania musi mieć możliwość sprawdzenia aktualnych wersji oprogramowania antywirusowego. |
| AV-76 | W całym okresie trwania subskrypcji użytkownik musi mieć prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej oraz pobierania nowych wersji oprogramowania zarządzającego. |

1. W przypadku zaoferowania przez wykonawcę oprogramowania antywirusowego innego, niż używane obecnie przez Zamawiającego (rozwiązania równoważnego), wykonawca zobowiązany jest dodatkowo do:
2. przeprowadzenia wspólnie z administratorami Zamawiającego, przed dniem dostawy oprogramowania, pełnej deinstalacji posiadanego przez Zamawiającego aktualnego oprogramowania antywirusowego ze wszystkich stacji roboczych i serwerów pracujących w sieci lokalnej Zamawiającego (konieczna jest fizyczna obecność wykwalifikowanego przedstawiciela Wykonawcy w siedzibie Zamawiającego), łącznie z usunięciem wpisów w rejestrach systemowych,
3. zainstalowania centralnego systemu zarządzania zaoferowanego oprogramowania oraz instalacji agentów na wszystkich stacjach roboczych i serwerach Zamawiającego z zastrzeżeniem, że nie będzie miał on uprawnień do uzyskania dostępu do przetwarzanych w CPPC danych osobowych, a przed rozpoczęciem czynności zobowiąże się do zachowania poufności, podpisując oświadczenie o poufności wg wzoru wskazanego przez Zamawiającego;
4. przeprowadzenia działań wymienionych w lit. a) i b) w godzinach pracy Zamawiającego,
5. zaoferowania oprogramowania o parametrach nie gorszych, niż obecnie używane przez Zamawiającego „ESET PROTECT Entry ON-PREM”. Zamawiający dokona oceny zaoferowanego oprogramowania równoważnego na podstawie złożonych przez wykonawcę wraz z ofertą przedmiotowych środków dowodowych, zgodnie z zapisami rozdziału X SWZ. Przedstawione dokumenty mają potwierdzać, że oferowany produkt spełniają wymagania w zakresie równoważności tj. minimalne wymagania dotyczące przedmiotu zamówienia, które zostały opisane w tabeli powyżej.
6. dostarczenia dokumentacji powdrożeniowej zaoferowanego rozwiązania w wersji papierowej oraz elektronicznej (pdf i doc) na cyfrowym nośniku danych (płyty CD, DVD, pamięć USB) wraz z opisem architektury logicznej systemu i graficzną prezentacją połączeń, specyfikację techniczną rozwiązania. Dokumentacja musi zawierać opis podstawowych procedur administracyjnych i utrzymaniowych, które są niezbędne do prawidłowej eksploatacji systemu. Dostarczona dokumentacja w wersji papierowej musi być parafowana przez wykonawcę na każdej stronie oraz podpisana na ostatniej,
7. zakończenia wdrożenia oprogramowania w nieprzekraczalnym terminie do 3 dni kalendarzowych od dnia podpisania Umowy, natomiast dostarczenia dokumentacji powdrożeniowej w terminie do 10 dni kalendarzowych od dnia podpisania Umowy,
8. dostarczenia produktów wskazanych w lit. a), b) i e) w terminach ustalonych wspólnie z Zamawiającym, z uwzględnieniem terminów określonych w lit. f). Ustalenie terminu dostarczenia produktów wskazanych w zdaniu poprzednim nastąpi nie później niż w następnym dniu roboczym po zawarciu umowy, przy użyciu poczty elektronicznej, na adresy e-mail wskazane w umowie.
9. W sytuacji, gdy oprogramowanie przedstawione w ofercie w momencie dostawy nie będzie dostępne na rynku, będzie wycofane ze sprzedaży przez producenta lub producent wprowadzi nową wersję oprogramowania, Zamawiający dopuszcza dostarczenie nowszej lub lepszej wersji oprogramowania, bez zmiany wynagrodzenia ustalonego w ofercie.
10. Jeżeli zaoferowane oprogramowanie antywirusowe nie będzie spełniało wymagań określonych w ust. 4 oferta będzie podlegać odrzuceniu.
11. Podane przez Zamawiającego nazwy (znaki towarowe) zamawianego przedmiotu zamówienia mają charakter przykładowy, a ich wskazanie ma na celu określenie oczekiwanego standardu zamawianego przedmiotu zamówienia, przy czym w każdym przypadku Zamawiający dopuszcza zaoferowanie produktu równoważnego, o nie gorszych parametrach, z zachowaniem wymagań określonych w OPZ.