|  |  |
| --- | --- |
| Parametr | Parametry oferowanego przedmiotu zamówienia  - należy określić rzeczywiste parametry oferowanego przez wykonawcę przedmiotu zamówienia; dopuszcza się wpisanie spełnia / nie spełnia ale zweryfikowanie wskazanego parametru musi być możliwe za pomocą załączonej do oferty karty technicznej produktu lub innego równoważnego dokumentu  - określenie poniższych parametrów nie zwalnia Wykonawcy ze spełnienia zapisów określonych w szczegółowym opisie przedmiotu zamówienia dla danej części. |
| Nazwa zaoferowanego oprogramowania antywirusowego |  |
| Ilość urządzeń objętych licencją oprogramowania antywirusowego |  |
| Możliwości instalacji serwera administracyjnego oprogramowania antywirusowego |  |
| Wymóg korzystania z zewnętrznej bazy danych przez serwer administracyjny oprogramowania antywirusowego |  |
| Wspierane sposoby instalacji bazy danych w przypadku wymogu korzystania z zewnętrznej bazy danych przez serwer administracyjny oprogramowania antywirusowego |  |
| Wspierane sposoby instalacji bazy danych w przypadku wymogu korzystania z zewnętrznej bazy danych przez serwer administracyjny oprogramowania antywirusowego |  |
| Wsparcie dla baz danych MS SQL i MySQL w przypadku wymogu korzystania z zewnętrznej bazy danych przez serwer administracyjny oprogramowania antywirusowego |  |
| Możliwość umiejscowienia bazy danych serwera administracyjnego oprogramowania antywirusowego na innym serwerze |  |
| Możliwość dostępu do konsoli centralnego zarządzania serwera administracyjnego oprogramowania antywirusowego w języku polskim z poziomu interfejsu WWW |  |
| Możliwość zabezpieczenia dostępu do konsoli centralnego zarządzania serwera administracyjnego oprogramowania antywirusowego z poziomu interfejsu WWW za pośrednictwem protokołu SSL |  |
| Zabezpieczenie komunikacji pomiędzy poszczególnymi modułami serwera administracyjnego oprogramowania antywirusowego za pomocą certyfikatów |  |
| Możliwość utworzenia własnego CA (Certification Authority) przez serwer administracyjny oprogramowania antywirusowego oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. |  |
| Możliwość zarządzania urządzeniami z systemem Android przez serwer administracyjny oprogramowania antywirusowego |  |
| Możliwość centralnej konfiguracji i zarządzania przynajmniej takimi modułami serwera administracyjnego oprogramowania antywirusowego jak ochrona antywirusowa i antyspyware, które działają na stacjach roboczych w sieci |  |
| Możliwość weryfikacji przez serwer administracyjny oprogramowania antywirusowego 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) |  |
| Możliwość instalowania i odinstalowywania oprogramowania firm trzecich dla systemów Windows oraz odinstalowywania oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT przez serwer administracyjny zaoferowanego oprogramowania antywirusowego |  |
| Możliwość tworzenia grup statycznych i dynamicznych komputerów w serwerze administracyjnym zaoferowanego oprogramowania antywirusowego |  |
| Możliwość tworzenia grup dynamicznych 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) w serwerze administracyjnym zaoferowanego oprogramowania antywirusowego |  |
| Zapewnienie przez serwer administracyjny zaoferowanego oprogramowania antywirusowego gotowych szablonów raportów, przygotowanych przez producenta oraz możliwości tworzenia własnych raportów przez administratora |  |
| Możliwość wysłania przez administratora serwera administracyjnego oprogramowania antywirusowego, powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog |  |
| Możliwość podziału uprawnień administratorów w serwerze administracyjnym oprogramowania antywirusowego w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami |  |
| Możliwość pobrania wszystkich wymaganych elementów serwera centralnej bezpośrednio ze strony producenta |  |
| Systemy operacyjne ze wsparciem oprogramowania antywirusowego oraz zakres tego wsparcia |  |
| Możliwość wykrywania i usuwania niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich i backdoor przez oprogramowanie antywirusowe |  |
| Zapewnienie przez oprogramowanie antywirusowe ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet |  |
| Wykrywanie przez oprogramowanie antywirusowe potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji |  |
| Możliwość skanowania przez oprogramowanie antywirusowe w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. |  |
| Możliwość skanowania przez oprogramowanie antywirusowe całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu |  |
| Możliwość skanowania przez oprogramowanie antywirusowe plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych |  |
| Możliwość umieszczenia w oprogramowaniu antywirusowym na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku |  |
| Brak konieczności ponownego uruchomienia (restartu) komputera po aktualizacji oprogramowania antywirusowego |  |
| Możliwość skanowania i oczyszczania poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym) przez oprogramowanie antywirusowe zanim zostanie ona dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego) |  |
| Możliwość skanowania przez oprogramowanie antywirusowe ruchu HTTP na poziomie stacji roboczych. |  |
| Możliwość automatycznego zablokowania zainfekowanego ruchu przez oprogramowanie antywirusowe i wyświetlania użytkownikowi stosowne powiadomienia |  |
| Możliwość skanowania ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS |  |
| Ilość modułów niezależnych modułów heurystycznych w jakie wyposażone jest oprogramowanie antywirusowe oraz wykorzystywane przez oprogramowanie metody heurystyczne |  |
| Możliwość wyboru z jaką heurystyką ma odbywać się skanowanie (z użyciem jednej lub wielu metod jednocześnie) w oprogramowaniu antywirusowym |  |
| Możliwość blokowania przez administratora zewnętrznych nośników danych na stacji roboczej z zainstalowanym oprogramowaniem antywirusowym, 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 |  |
| Możliwość tworzenia reguł dla urządzeń podłączanych do stacji roboczej z oprogramowaniem antywirusowym minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia |  |
| Możliwość utworzenia reguły na podstawie urządzenia podłączonego do stacji roboczej z zainstalowanym oprogramowaniem antywirusowym (dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia) |  |
| Możliwość nadania przez użytkownika oprogramowania antywirusowego uprawnień dla podłączanych urządzeń, w tym co najmniej: dostępu w trybie do odczytu, pełnego dostępu, ostrzeżenia, brak dostępu do podłączanego urządzenia |  |
| Tryby pracy modułu HIPS oprogramowania antywirusowego |  |
| Możliwość wygenerowania przez oprogramowanie antywirusowe pełnego raportu na temat stacji, na której został zainstalowany, 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 (funkcja, generująca taki log, ma posiadać różne poziomy filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa) |  |
| Możliwość automatycznej, inkrementacyjnej aktualizacja silnika detekcji oprogramowania antywirusowego |  |
| Ilość procesów uruchamianych przez oprogramowanie antywirusowe w pamięci |  |
| Możliwość ochrony użytkownika oprogramowania antywirusowego poprzez wykrywanie i blokowanie zagrożeń atakujących jeszcze przed uruchomieniem systemu operacyjnego (funkcjonalność skanera UEFI) |  |
| Brak dodatkowego interfejsu graficznego dla wbudowanego w oprogramowanie antywirusowe skanera UEFI i jego transparentność dla użytkownika, aż do momentu wykrycia zagrożenia |  |
| Wyposażenie oprogramowania antywirusowego w zintegrowany moduł kontroli dostępu do stron internetowych |  |
| Możliwość utworzenia reguł oprogramowania antywirusowego w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory |  |
| Ilość kategorii i podkategorii w oparciu o które można filtrować adresy URL w oprogramowaniu antywirusowym |  |
| Wyposażenie oprogramowania antywirusowego w co najmniej następujące kategorie: materiały dla dorosłych, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, aktualności, polityka, prawo, wyszukiwarki, bezpieczeństwo, szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, serwery proxy, alkohol i tytoń, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii |  |
| Możliwość automatycznej aktualizacji przez producenta oprogramowania antywirusowego listy adresów URL znajdujących się w poszczególnych kategoriach |  |
| Możliwość pełnej ochrony użytkownika oprogramowania antywirusowego przed wirusami, trojanami, robakami i innymi zagrożeniami |  |
| Możliwość wykrywania i usuwania przez oprogramowanie antywirusowe niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor |  |
| Wbudowana w oprogramowanie antywirusowe technologia do ochrony przed rootkitami i exploitami |  |
| Możliwość wykorzystania przez oprogramowanie antywirusowe wielu wątków skanowania w przypadku maszyn wieloprocesorowych |  |
| Wsparcie przez oprogramowanie antywirusowe mechanizmu klastrowania |  |
| Zapewnienie przez oprogramowanie antywirusowe systemu zapobiegania włamaniom działający na hoście (HIPS). |  |
| Możliwość skanowania dysków sieciowych typu NAS przez zaoferowane oprogramowanie sieciowe |  |
| Możliwość blokowania zewnętrznych nośników danych na serwerze plików zabezpieczonym oprogramowaniem antywirusowym 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 |  |
| Możliwość automatycznego wykrywania przez oprogramowanie antywirusowe usług zainstalowanych na serwerze i automatycznego tworzenia dla nich odpowiednich wyjątków |  |
| Możliwość automatycznego dodawania kolejnych wyłączeń w systemie ochrony oprogramowania antywirusowego w przypadku zainstalowania na serwerze nowych usług serwerowych (funkcja ta nie może wymagać restartu serwer, a automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych) |  |
| Możliwość zmiany konfiguracji oprogramowania antywirusowego oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line) |  |
| Wsparcie przez system antywirusowy skanowania magazynu Hyper-V |  |
| Możliwość wykluczania procesów ze skanowania przez program antywirusowy |  |
| Zapewnienie przez oprogramowanie antywirusowe wbudowanego systemu IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych |  |
| Możliwość dodawania przez administratora oprogramowania antywirusowego wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP |  |
| Możliwość ochrony przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu oprogramowania antywirusowego |  |
| Możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta oprogramowania antywirusowego (w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty) |  |
| Możliwość wyłączenia z przesyłania do analizy przez producenta oprogramowania antywirusowego określonych plików i folderów |  |
| Możliwość uwierzytelnienia przez oprogramowanie antywirusowe użytkownika zanim zostanie uruchomiony system operacyjny (musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia) |  |
| Szyfrowanie pełnej powierzchni dysku przez oprogramowanie antywirusowe musi umożliwiać wykorzystanie modułu TPM. |  |
| Możliwość korzystania z technologii TCG OPAL przez oprogramowanie antywirusowe (dyski sprzętowo szyfrowane) |  |
| Możliwość zarządzania aplikacją do szyfrowania z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej |  |
| Możliwość wygenerowania przez konsolę centralnego zarządzania oprogramowania antywirusowego, dysku ratunkowego dla każdej zaszyfrowanej stacji |  |
| Możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych z zainstalowanym oprogramowaniem antywirusowym, w oparciu o przynajmniej: ilość znaków, warunek czy hasło ma zawierać wielkie litery,  warunek czy hasło ma zawierać małe litery, warunek czy hasło ma zawierać cyfry, warunek czy hasło ma zawierać znaki specjalne, okres ważności, ilość nieudanych logowań, możliwość zmiany hasła |  |
| Możliwość ograniczenia wyświetlania interfejsu graficznego oprogramowania antywirusowego użytkownikom komputera |  |
| Możliwość zablokowania dostępu do zaszyfrowanego dysku przez administratora oprogramowania antywirusowego |  |
| Wyposażenie programu antywirusowego w moduł bezpiecznej przeglądarki automatycznie szyfrującej wszelkie dane wprowadzane przez użytkownika |  |
| Możliwość automatycznego przekierowania użytkownika w momencie wejścia na stronę, która znajduje się na liście chronionych witryn |  |
| Możliwość konfiguracji przez administratora oprogramowania antywirusowego listy witryn chronionych przez bezpieczną przeglądarkę |  |
| Zapewnienia przez oprogramowanie antywirusowe ochrony przed zagrożeniami 0-day |  |
| Wykorzystywanie przez oprogramowanie antywirusowe do działania chmury producenta |  |
| Możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie przez oprogramowanie antywirusowe (w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi) |  |
| Możliwość zdefiniowania po jakim czasie przesłane przez oprogramowanie antywirusowe pliki muszą zostać usunięte z serwerów producenta |  |
| Możliwość zdefiniowania maksymalnego rozmiaru przesyłanych do chmury przez oprogramowanie antywirusowe próbek |  |
| Możliwość utworzenia listy wykluczeń określonych plików lub folderów z przesyłania do chmury przez oprogramowanie antywirusowe |  |
| Przesyłanie przez oprogramowanie antywirusowe po zakończonej analizie pliku w chmurze wyników analizy do wszystkich wspieranych produktów |  |
| Możliwość podejrzenia w programie antywirusowym listy plików, które zostały przesłane do analizy |  |
| Możliwość analizowania plików przez oprogramowanie antywirusowe bez względu na lokalizacje stacji roboczej (w przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione) |  |
| Brak wymogu instalacji dodatkowego agenta na stacjach roboczych na potrzeby usługi Sanbox w chmurze oprogramowania antywirusowego |  |
| Możliwość wysłania dowolnej próbki do analizy w chmurze przez użytkownika lub administratora za pomocą oprogramowania antywirusowego |  |
| Możliwość podejrzenia w programie antywirusowym jakie pliki zostały wysłane do analizy oraz przez kogo |  |
| Nazwa licencji zaoferowanej dla oprogramowania antywirusowego |  |
| Okres korzystania przez Zamawiającego z aktualizacji oprogramowania antywirusowego, baz wirusów itp. |  |
| Okres korzystania przez Zamawiającego z usług opartych o serwery producenta jak np. sandbox w przypadku zaoferowania oprogramowania z funkcjonalnością opartą o serwery producenta |  |
| Dostępność pierwszej linii wsparcia technicznego w języku polskim w trybie 8x5 |  |

**Lista dokumentów które muszą zostać załączone do formularza oferty**

(dokumenty muszą być wystawione w języku polskim lub angielskim)

1. Karta produktowa umożliwiającą weryfikację parametrów oferowanego oprogramowania lub inny równoważny dokument
2. Certyfikat ISO 9001 w zakresie świadczenia usług serwisowych wystawiony dla Wykonawcy
3. Certyfikat techniczny producenta oprogramowania wystawiony dla co najmniej jednego inżyniera technicznego zatrudnionego przez Wykonawcę