Załącznik nr 4 do SWZ - Zestawienie asortymentowo-ilościowe oraz parametry wymagane

.....
Nazwa i adres Wykonawcy:

UWAGA! Zamawiający infromuje, że parametry i warunki określone w kolumnie "Kryterium wymagalności" - określone jako "TAK" są parametrami wymaganymi przez Zamawiającego. Zamawiajacy wymaga spełnienia każdego z parametrów/warunków wymaganych w złożonej ofercie. Brak informacji w kolumnie "PARAMETR OFEROWANY" o danym parametrze/warunku oznaczać będzie jako brak zaoferowania tego parametru/warunku przez Wykonawcę. Niespełnienie nawet jednego z wymaganych parametrów/warunków spowoduje odrzucenie oferty.

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym zgodnie z art. 275 pkt 1 ustawy PZP, na zakup, dostawę, instalację oraz wdrożenie systemu ochrony antywirusowej dla Szpitala Wojewódzkiego im. Kardynała Stefana Wyszyńskiego w Łomży, znak sprawy: ZT-SZP-226/01/67/2022
OFERUJEMY

Lp.	Opis Przedmiotu zamówienia		Kryterium wymagalności	PARAMETR OFEROWANY - *(wypełnia Wykonawca)* *Uwaga ! Należy wypełnić dla każdgo parametru i szczegółowo opisać.*
1	Pełna nazwa oferowanego systemu ochrony antywirusowej z zaporą ogniową oraz w pełni zarządzalną centralną konsolą zarządzającą systemem **dla 700 szt. stacji roboczych i serwerów oraz 55 szt. urządzeń mobilnych** (w tym nazwa, wersja oferowanego systemu).		TAK, podać	
2	System musi umożliwiać ochronę antywirusową stacji roboczych:		TAK	
		- Microsoft Windows 7 (32/64-bit);	TAK	
		- Microsoft Windows 8.1 (32/64-bit);	TAK	
		- Microsoft Windows 10 (32/ 64-bit);	TAK	
		- Microsoft Windows 11 (32/ 64-bit).	TAK	
3	System musi umożliwiać ochronę antywirusową serwerów:		TAK	
		- Microsoft Windows Server 2008 R2;	TAK	
		- Microsoft Small Business Server 2011, Standard Edition;	TAK	
		- Microsoft Small Business Server 2011, Essentials;	TAK	
		- Microsoft Windows Server 2012;	TAK	
		- Microsoft Windows Server 2012 Essentials;	TAK	
		- Microsoft Windows Server 2012 R2;	TAK	
		- Microsoft Windows Server 2012 R2 Essentials;	TAK	
		- Microsoft Windows Server 2012 R2 Foundation;	TAK	
		- Microsoft Windows Server 2016 Standard;	TAK	
		- Microsoft Windows Server 2016 Essentials;	TAK	
		- Microsoft Windows Server 2016 Datacenter;	TAK	
		- Microsoft Windows Server 2016 Core;	TAK	
		- Microsoft Windows Server 2019 Standard;	TAK	
		- Microsoft Windows Server 2019 Essentials;	TAK	
		- Microsoft Windows Server 2019 Datacenter;	TAK	
		- Microsoft Windows Server 2019 Core;	TAK	
		- Microsoft Windows Server 2022 Standard;	TAK	
		- Microsoft Windows Server 2022 Essentials;	TAK	
		- Microsoft Windows Server 2022 Datacenter;	TAK	
		- Microsoft Windows Server 2022 Core.	TAK	
4	System musi umożliwiać ochronę antywirusową serwerów terminalowych:		TAK	
		- Microsoft Windows Terminal/RDP Services;	TAK	
		- Citrix XenApp 5.0;	TAK	
		- Citrix XenApp 6.0;	TAK	
		- Citrix XenApp 6.5;	TAK	
		- Citrix XenApp 7.0 - 7.15.	TAK	
5	Ochrona antywirusowa wyżej wymienionego systemu musi umożliwiać monitorowanie i zarządzanie systemem z pojedynczej, centralnej konsoli.		TAK	
6	Komunikacja ochrony antywirusowej z serwerem zarządzania musi odbywać się za pomocą protokołu HTTPS.		TAK	
7	Możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach.		TAK	
8	Polski interfejs użytkownika aplikacji ochronnej.		TAK	
Wymagania technologiczne do systemu antywirusowego:				
9	Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz modułu antyrootkit i modułu antyransonmware.		TAK	
10	Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.		TAK	
11	Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan".		TAK	

12	Instalator oprogramowania na stacji końcowej musi sprawdzać istnienie poprzednich wersji oprogramowania oraz oprogramowania uniemożliwiającego poprawne działanie klienta.	TAK	
13	W przypadku znalezienia poprzedniej wersji oprogramowania antywirusowego instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie klienta stacji końcowej lub serwera zarządzania i instalować nowe wersję.	TAK	
14	W przypadku znalezienia oprogramowania uniemożliwiającego poprawne działanie klienta, instalator powinien poinformować o tym użytkownika i w razie akceptacji usunąć takie oprogramowanie.	TAK	
15	Możliwość zdefiniowania automatycznego procesu usuwania oprogramowania uniemożliwiającego poprawne działanie klienta, bez informowania użytkownika końcowego.	TAK	
16	Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa musi być zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.	TAK	
17	Możliwość dystrybuowania aktualizacji baz definicji wirusów, aktualizacji oprogramowania zainstalowanego na stacji końcowej, oraz polityk bezpieczeństwa za pomocą serwera pośredniczącego. Serwer pośredniczący pobiera aktualizacje oprogramowania, jak i bazy antywirusowe, z serwerów producenta, a następnie dystrybuuje je w sieci lokalnej.	TAK	
18	Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.	TAK	
19	Możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.	TAK	
20	Możliwość wywołania skanowania po uruchomieniu systemu operacyjnego, oraz po zalogowaniu użytkownika.	TAK	
21	Możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.	TAK	
22	Możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.	TAK	
23	Możliwość skanowania dysków przenośnych takich jak dyski USB, dyski zewnętrzne, drukarki czy dyski sieciowe.	TAK	
24	Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.	TAK	
25	Skanowanie na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym.	TAK	
26	Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).	TAK	
27	Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.	TAK	
28	Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.	TAK	
29	Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit" oraz ataki typu 0-day.	TAK	
30	Mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne (przez pliki wykonywalne rozumie się co najmniej: aplikacje, interpretowalną zawartość Flash, Sliverlight, skrypty oraz makra dokumentów pakietu Office).	TAK	
31	Technologia wykrywania nowych i nieznanych zagrożeń typu 0-day, powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie mogą być wysyłane do analizy w infrastrukturze producenta.	TAK	
32	Technologia wykrywania nowych i nieznanych zagrożeń, powinna w przypadku podejrzanych plików umożliwiać automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.	TAK	
33	Możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.	TAK	
34	Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie.	TAK	
35	Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.	TAK	
36	Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP, JAR, ARJ, LZH, TAR, TGZ, GZ, CAB, RAR, BZ2, HQX.	TAK	
37	Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.	TAK	
38	Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.	TAK	
39	Automatyczne uruchamianie procedur naprawczych.	TAK	
40	Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.	TAK	
41	Automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem stacja robocza jest odpowiednio zabezpieczona.	TAK	
42	Możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.	TAK	

43	Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.	TAK	
44	Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.	TAK	
45	Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.	TAK	
46	Ochrona przeglądarki internetowej, w tym: analiza uruchamianych skryptów ActiveX i pobieranych plików.	TAK	
47	Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie *Network Interceptor Framework* (niezależnie od rodzaju i wersji przeglądarki).	TAK	
48	Możliwość zabezpieczenia połączenia do witryn skategoryzowanych przez producenta, jako 'bankowość elektroniczna' poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z bankiem.	TAK	
49	Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z daną witryną HTTPS.	TAK	
50	Możliwość blokowania uruchomienia aplikacji na stacji końcowej.	TAK	
51	Blokowanie możliwości uruchomienia aplikacji na stacji końcowej musi umożliwiać identyfikację aplikacji, co najmniej na podstawie identyfikatora SHA1.	TAK	
52	Możliwość zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.	TAK	
53	Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.	TAK	
54	Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).	TAK	
55	Blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy reputacyjne producenta. Brak konieczności ręcznego wpisywania poszczególnych adresów.	TAK	
56	Oprogramowanie musi zapewnić co najmniej 30 kategorii klasyfikacji witryn WWW.	TAK	
57	Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, musi zostać powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.	TAK	
58	Możliwość blokowania witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.	TAK	
59	Brak konieczności restartu systemu operacyjnego po zainstalowaniu aplikacji w środowisku Windows 7/8/8.1/10/11.	TAK	
60	Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi odbywać się w formie zaszyfrowanej.	TAK	
61	Moduł aktualizatora aplikacji, który okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.	TAK	
62	Aktualizator aplikacji musi spełniać role programu łatającego podatności i instalującego aktualizacje oprogramowania, a nie tylko i wyłącznie pasywnego skanera luk w bezpieczeństwie aplikacji.	TAK	
63	Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.	TAK	
64	System centralnego zarządzania musi prezentować niezaktualizowane aplikacje na komputerach dotyczące całej domeny lub listę nieaktualizowane oprogramowania dla pojedynczej stacji końcowej.	TAK	
65	Aktualizator aplikacji nie może wymagać instalowania dodatkowych agentów oprócz agenta AV (systemu antywirusowego).	TAK	
66	Aktualizator powinien dać możliwość wymuszenia instalacji aktualizacji w sposób akcji wymuszonej z poziomu interfejsu zarządzania lub reguły wykonującej się w sposób zaplanowany: dzień, godzina, opcje restartu komputera, wykluczenia aplikacji.	TAK	
67	Administrator konsoli zarządzającej musi mieć możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.	TAK	
68	Aktualizator aplikacji nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.	TAK	
69	Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.	TAK	
70	Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.	TAK	
71	Istnieje możliwość blokady zapisywania plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta musi umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.	TAK	

72	Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.		TAK	
73	Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.		TAK	
74	Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.		TAK	
75	Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.		TAK	
76	Wsparcie Antimalware Scan Interface (AMSI).		TAK	
77	Możliwość ukrycia programu z zasobnika systemowego dla użytkowników końcowych.		TAK	
78	Ochrona plików programu przed naruszeniem		TAK	
79	Możliwość ustalenia hasła, które umożliwia zwolnienie plików z kwarantanny przez użytkownika, bądź całkowite zakazanie zwolnienia z kwarantanny.		TAK	
Ochrona urządzeń Mac				
80	Ochrona antywirusowa komputerów musi komunikować się z systemem centralnego zarządzania oprogramowaniem AV.		TAK	
81	Oprogramowanie musi być kompatybilne z następującymi systemami operacyjnymi:		TAK	
		- mac OS 10.15 Catalina	TAK	
		- mac OS 10.14 Mojave	TAK	
		- mac OS 10.13 High Sierra	TAK	
		- mac OS 11.0 Big Sur	TAK	
Ochrona urządzeń mobilnych z systemami Android, iOS i iPadOS				
82	Ochrona antywirusowa urządzeń mobilnych musi komunikować się z systemem centralnego zarządzania oprogramowaniem AV.		TAK	
83	Oprogramowanie musi być kompatybilne z mobilnymi systemami operacyjnymi:		TAK	
		- Android 7.0 i wyższe wersje	TAK	
		- iOS 12.1 i wyższe wersje	TAK	
		- iPadOS 13 i wyższe wersje.	TAK	
84	W ramach oferowanych **755 szt. licencji na urządzenia, min. 55 szt. licencj**i musi być dedykowanych dla urządzeń mobilnych z systemami operacyjnymi opisanymi w pkt. 83 powyżej o ile producent oferowanego systemu traktuje urządzenia mobilne oddzielnie.		TAK, podać	
85	Aplikacja na urządzenia mobilne musi wspierać działanie z rozwiązaniami MDM co najmniej: AirWatch, IBM MaaS360, Google MDM, Microsoft Intune, Miradore, MobileIron.		TAK	
86	Wdrożenie oprogramowania ma działać na zasadzie zaproszeń e-mail wysyłanych do użytkowników końcowych.		TAK	
87	Program musi zawierać funkcjonalność ochrony przeglądania zapobiegającą odwiedzaniu szkodliwych stron internetowych, także z wsparciem HTTPS.		TAK	
88	Aplikacja musi posiadać funkcjonalność VPN z możliwością wyboru wirtualnej lokalizacji sieciowej z możliwością ograniczenia listy lokacji przez administratora.		TAK	
89	Wspierane lokacje VPN to co najmniej: Espoo, Sztokhol, Oslo, Kopenhaga, Madryt, Warszawa, Paryż, Bruksela, Amsterdam, Milan, Falkenstein, Londyn, Wschodnie wybrzeżę USA, Zachodnie wybrzeże USA, Montreal, Tokyo, Melborune.		TAK	
90	Administrator musi posiadać możliwość wybrania aplikacji które pomijają VPN.		TAK	
91	Dla systemów firmy Apple administrator musi posiadać możliwość wyboru protokołu VPN między IKEv1, IKEv2 bądź wybór automatyczny.		TAK	
92	Produkt musi zawierać funkcjonalność Anti-Tracking, która zapobiega śledzeniu przez reklamodawców, oraz przez pliki cookie.		TAK	
93	Dla systemu Android produkt musi zawierać lekki moduł ochrony przed złośliwym oprogramowaniem, który blokuje wirusy, malware oraz wykrywa ransomware.		TAK	
94	Administrator musi posiadać możliwość regulowania skanowania w wypadku połączenia sieciowego z limitem użycia danych.		TAK	
95	Administrator musi posiadać możliwość zaplanowania skanowania antywirusowego w czasie codziennym, co tydzień, co cztery tygodnie bądź miesięcznie.		TAK	
96	Administrator musi posiadać możliwość zablokowania każdej opcji konfiguracyjnej przed modyfikacją przez użytkownika.		TAK	
System centralnego zarządzania:				
97	System centralnego zarządzania w języku polskim.		TAK	
98	System centralnego zarządzaniamusi mieć możliwość zainstalowania na wersjach serwerowych Microsoft Windows lub Linux.		TAK	

99	Instalacja sytemu centralnego zarządzania dla Microsoft Windows musi wspierać następujące wersje systemów operacyjnych:		TAK	
		- Windows Server 2008 SP1 64-bit: Standard, Enterprise, Web Server, Small Business Server, Essential Business Server;	TAK	
		- Windows Server 2008 R2: Standard, Enterprise, Web Server;	TAK	
		- Windows Server 2012: Essentials, Standard, Datacenter;	TAK	
		- Windows Server 2012 R2: Essentials, Standard, Datacenter;	TAK	
		- Windows Server 2016 Essentials, Standard, Datacenter;	TAK	
		- Windows 2019 Essentials, Standard, Datacenter;	TAK	
		- Windows 2022 Essentials, Standard, Datacenter.	TAK	
100	Instalacja sytemu centralnego zarządzania dla Linux musi wspierać następujące wersje systemów operacyjnych:		TAK	
		- Red Hat Enterprise Linux 6 32/64-bit;	TAK	
		- Red Hat Enterprise Linux 7 32/64-bit;	TAK	
		- Red Hat Enterprise Linux 8 32/64-bit;	TAK	
		- CentOS 6 32/64-bit;	TAK	
		- CentOS 7 32/64-bit;	TAK	
		- CentOS 8 32/64-bit;	TAK	
		- SuSE Linux Enterprise Server 11 32/64-bit;	TAK	
		- SuSE Linux Enterprise Server 12 32/64-bit;	TAK	
		- SuSE Linux Enterprise Server 15 32/64-bit;	TAK	
		- SuSE Linux Enterprise Desktop 11, 12, 15 32/64-bit;	TAK	
		- openSUSE Leap 43.15 32/64-bit;	TAK	
		- Debian GNU Linux 8 (Jessie) 32/64-bit;	TAK	
		- Debian GNU Linux 9 (Stretch) 32/64-bit;	TAK	
		- Ubuntu 14.04 (Trusty Tahr) 32/64-bit;	TAK	
		- Ubuntu 16.04 (Xenial Xerus) 32/64-bit;	TAK	
		- Ubuntu 18.04 (Bionic Beaver) 32/64-bit;	TAK	
		- Ubuntu 20.04 (Focal Fossa) 32/64-bit;	TAK	
		- Oracle Linux 8.	TAK	
101	System centralnego zarządzania musi wspierać następujące przeglądarki internetowe do obsługi konsoli zarządzającej:		TAK	
		- Microsoft Edge	TAK	
		- Mozilla Firefox	TAK	
		- Google Chrome	TAK	
		- Safari.	TAK	
102	Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.		TAK	
103	Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.		TAK	
104	Wykresy są interaktywne, tzn. że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.		TAK	
105	Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.		TAK	
106	Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.		TAK	
107	Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.		TAK	
108	Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem).		TAK	
109	Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi.		TAK	
110	Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta.		TAK	
111	Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.		TAK	
112	Centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy.		TAK	
113	Możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów).		TAK	

114	Tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach.	TAK	
115	Możliwość importu struktury drzewa z Microsoft Active Directory.	TAK	
116	Możliwość tworzenia reguł synchronizacji z Microsoft Active Directory umożliwiających automatyczną synchronizację klientów z aktualnie istniejącymi grupami komputerów.	TAK	
117	Możliwość tworzenia reguł powiadamiania o nowych, niezarządzanych klientach w Microsoft Active Directory.	TAK	
118	Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników.	TAK	
119	Możliwość zdefiniowania hasła do odinstalowania aplikacji.	TAK	
120	Możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający.	TAK	
121	Możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji.	TAK	
122	Możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta.	TAK	
123	Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania. Dane muszą być przesyłane do serwera zarządzania podczas kolejnego połączenia.	TAK	
124	Możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.	TAK	
125	Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.	TAK	
126	Profile mogą być przypisane do pojedynczych hostów lub do grup.	TAK	
127	Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.	TAK	
128	Tworzone profile muszą dawać administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.	TAK	
129	W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.	TAK	
130	Umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe.	TAK	
131	Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej, niż co 7 dni (zalecane codzienne aktualizacje).	TAK	
132	Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe.	TAK	
133	Możliwość eksportu raportów z pracy systemu do pliku HTML.	TAK	
134	Możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich.	TAK	
135	Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”.	TAK	
136	Program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa.	TAK	
137	Program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe.	TAK	
138	Dedykowany system raportowania dostępny przez przeglądarkę internetową umożliwiający podgląd statystyk dotyczących wykrytych wirusów, przeprowadzonych ataków, zainstalowanego oprogramowania oraz statystyk połączenia stacji klienckich.	TAK	
139	System raportowania umożliwiający wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora.	TAK	
140	Zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania.	TAK	

141	Możliwość przekierowania alertów bezpośrednio do serwera Syslog.		TAK	
142	Możliwość tworzenia wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).		TAK	
143	System umożliwiający wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączania programu.		TAK	
144	Możliwość wykonywania automatycznej kopii bazy danych systemu zarządzania centralnego zgodnie z harmonogramem określonym przez administratora.		TAK	
145	Możliwość określenia liczby kopii bazy danych, jaka będzie przetrzymywana przez automatyczny system tworzenia kopii zapasowej.		TAK	
146	Możliwość wygenerowania danych diagnostycznych z podpiętych komputerów za pomocą konsoli zarządzającej.		TAK	
147	Możliwość bezpośredniego pobrania z komputera danych diagnostycznych z poziomu konsoli zarządzającej.		TAK	
148	Możliwość komentowania stosowanej konfiguracji stacji końcowych za pomocą notatek umieszczonych w interfejsie graficznym konsoli zarządzającej.		TAK	
149	Wsparcie REST API dla integracji z rozwiązaniami monitorowania i raportowania.		TAK	
Wymagania dodatkowe				
150	Zamawiający wymaga, aby zaproponowany produkt przez Wykonawcę posiadał w teście AVtest punktacje na poziomie 18 punktów za miesiące: maj 2022 r, czerwiec 2022 r liczony każdy oddzielnie		TAK, podać	
151		Niezależne testy (źródło) - https://www.av-test.org/en/antivirus/business-windows-client/	TAK	
152	Wykonawca zapewni okres usługi wsparcia technicznego od daty aktywacji klucza licencyjnego na okres 12 m-cy		TAK	
153	W ramach gwarancji i wsparcia technicznego Wykonawca, po zatwierdzeniu przez Zamawiającego, będzie dokonywał aktualizacji (rozumianych jako aktualizacje w ramach eksploatacji systemu np. wersji używanych bibliotek) niezbędnych napraw, korekt i uzupełnień Systemu przywracających jego pełną funkcjonalność.		TAK	
154	Wykonawca zapewni wsparcie techniczne przez mail / telefon w systemie 24/7 z czasem reakcji 4h w języku polskim świadczone przez producenta lub autoryzowanego dystrybutora		TAK, podać	
155	Okno serwisowe, w trakcie którego Wykonawca ma prawo wykonywać prace serwisowe na środowisku produkcyjnym zostaje określone od 19:00 do 07:00. Prace będą mogły być prowadzone po uprzednim potwierdzeniu terminu wykonania przez Zamawiającego.		TAK	
156	Wykonawca zapewni 4 wizyty serwisowe na miejscu u Zamawiającego, którego celem będzie sprawdzenie instalacji / konfiguracji i zgodności produktu z najlepszymi praktykami.		TAK	
157	Wykonawca zapewni na czas wdrożenia przynajmniej jednego inżyniera z certyfikatem potwierdzającym znajomość konsoli produktu w zakresie instalacji, konfiguracji i znajomości dobrych praktyk		TAK	
158	Wykonawca zapewni na czas wdrożenia przynajmniej jednego inżyniera posiadającego certyfikat ze znajomości oferowanego systemu/produktu i dobrych praktyk na poziomie rozszerzonym/zaawansowanym		TAK	
159	Wykonawca zapewni na czas wdrożenia przynajmniej jednego inżyniera z 3 letnim doświadczeniem jako inżynier oferowanego produktu.		TAK	
160	Wykonawca zobowiązuje się w czasie wdrożenia do przeniesienia wszystkich zaimplementowanych polityk z obecnego systemu antywirusowego do zaoferowanego oprogramowania		TAK	