



Szpital Specjalistyczny Nr 2 w Bytomiu
Jednostka ochrony zdrowia Samorządu Województwa Śląskiego

 **Śląskie.**



Fundusze
Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Zn. sprawy: 9/9PN/2022

Bytom, dnia 22.04.2022 r.

WYKONAWCY

ubiegający się o zamówienie publiczne

ZAWIADOMIENIE O MODYFIKACJI SIWZ

Dotyczy: Dostawa sprzętu dla realizowanego projektu „eCareMed - eZdrowie w Szpitalu Specjalistycznym Nr 2 w Bytomiu.

Szanowni Państwo,

Zamawiający informuje, iż zmodyfikował zapisy w załączniku nr 7 – Opis przedmiotu Zamówienia w ramach części:

- Załącznik nr 7 – Część nr 1 – Dostawa zestawu komputerów stacjonarnych wraz z systemem operacyjnym i pakietem oprogramowania biurowego – 200sztuk
- Załącznik nr 7 – Część nr 2 – Dostawa komputerów przenośnych wraz z systemem operacyjnym – 10sztuk.

Załącznik nr 7 - Część 1 - Opis przedmiotu zamówienia - Komputery stacjonarne:

Poprzedni opis:

Lp.	Oprogramowanie antywirusowe	Nazwa/oznaczenie:
	Ochrona antywirusowa	
99.	Producent:	

41-902 Bytom. ul. S. Batorego 15; NIP: 6262511259; REGON: 270235892
TEL.: 32 786-16-42; FAX: 32 786-16-46;
STRONA WWW: www.szpital2.bytom.pl; E-MAIL: sekretariat@szpital2.bytom.pl



Fundusze
Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



100.	Typ/Model	
101.	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami	
102.	Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.	
103.	Wbudowana technologia do ochrony przed rootkitami.	
104.	Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	
105.	Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie”.	
106.	Skanowanie „na żądanie” pojedynczych plików lub katalogów	
107.	Możliwość skanowania dysków sieciowych i dysków przenośnych.	
108.	Możliwość umieszczenia na liście wykluczenia ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach i procesów.	
109.	Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej za pomocą czytników (oprogramowania do obsługi poczty) email.	
110.	Skanowanie i oczyszczanie poczty przychodzącej POP3 „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).	
111.	Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.	
112.	Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.	
113.	Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator.	
114.	Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.	
115.	Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.	
116.	Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora	
117.	Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń	
118.	Możliwość obsługi pobierania aktualizacji za pośrednictwem serwera proxy.	

Fundusze Europejskie
Program RegionalnyRzeczpospolita
Polska

Śląskie.

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego

119.	Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.	
120.	Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.	
121.	Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie urządzenie)	
122.	Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, z bazy danych urządzeń podłączanych przez użytkowników do komputerów.	
123.	Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.	
124.	Jedna wersja instalacyjna na stacje robocze i serwery plików.	
125.	Wbudowana zaporą osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.	
126.	Możliwość tworzenia list sieci zaufanych.	
127.	Możliwość dezaktywacji funkcji zapory sieciowej	
128.	Hypervisor Introspection	
129.	Dla systemu Android możliwość blokowania stron internetowych.	
130.	Możliwość szyfrowania urządzenia opartego o system android.	
131.	Możliwość skanowania aplikacji w trakcie instalacji na urządzeniach z systemem Android	
	Oprogramowanie antywirusowe - Konsola zarządzająca	
132.	Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows, zdalna instalacja na środowiskach wirtualnych.	
133.	Możliwość integracji z kontem Domenowym Active Directory	
134.	Centralna konfiguracja i zarządzanie ochroną antywirusową antyspyware'ową oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych z jednego serwera zarządzającego.	
135.	Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.	
136.	Możliwość sprawdzenia z centralnej konsoli zarządzającej Stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie,	

	Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).	
137.	Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.	
138.	Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.	
139.	Możliwość zmiany konfiguracji na stacjach i serwerach jedynie z centralnej konsoli zarządzającej.	
140.	Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.	
141.	Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu min: pdf, csv	
142.	Raport generowany według harmonogramu z możliwością automatycznego wysłania go do Osób zdefiniowanych w tym raporcie.	
143.	Możliwość dezinstalacji oprogramowania antywirusowego innych firm.	
144.	Tworzenie osobnych polityk dla fizycznych komputerów, urządzeń mobilnych oraz maszyn wirtualnych.	
145.	Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci lub z ustawieniami niestandardowymi.	
146.	Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.	
147.	Uwierzytelnianie dwuskładnikowe	
148.	Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji	

Zmodyfikowany Opis:

Lp.	Oprogramowanie antywirusowe	Nazwa/oznaczenie:
	Ochrona antywirusowa	
99.	Producent:	
100.	Typ/Model	
101.	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami	

102.	Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.	
103.	Wbudowana technologia do ochrony przed rootkitami.	
104.	Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	
105.	Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie”.	
106.	Skanowanie „na żądanie” pojedynczych plików lub katalogów	
107.	Możliwość skanowania dysków sieciowych i dysków przenośnych.	
108.	Możliwość umieszczenia na liście wykluczenia ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach i procesów.	
109.	Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej za pomocą czytników (oprogramowania do obsługi poczty) email.	
110.	Skanowanie i oczyszczanie poczty przychodzącej POP3 „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej] (niezależnie od konkretnego klienta pocztowego).	
111.	Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.	
112.	Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.	
113.	Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator.	
114.	Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.	
115.	Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.	
116.	Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora	
117.	Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń	
118.	Możliwość obsługi pobierania aktualizacji za pośrednictwem serwera proxy.	
119.	Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.	
120.	Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.	

Fundusze Europejskie
Program RegionalnyRzeczpospolita
Polska

Śląskie.

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego

121.	Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie urządzenie)	
122.	Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, z bazy danych urządzeń podłączanych przez użytkowników do komputerów.	
123.	Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.	
124.	Jedna wersja instalacyjna na stacje robocze i serwery plików.	
125.	Wbudowana zaporą osobista, umożliwiającą tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.	
126.	Możliwość tworzenia list sieci zaufanych.	
127.	Możliwość dezaktywacji funkcji zapory sieciowej	
	Oprogramowanie antywirusowe - Konsola zarządzająca	
128.	Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows, zdalna instalacja na środowiskach wirtualnych.	
129.	Możliwość integracji z kontem Domenowym Active Directory	
130.	Centralna konfiguracja i zarządzanie ochroną antywirusową antyspyware'ową oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych z jednego serwera zarządzającego.	
131.	Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.	
132.	Możliwość sprawdzenia z centralnej konsoli zarządzającej Stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).	
133.	Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.	
134.	Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.	
135.	Możliwość zmiany konfiguracji na stacjach i serwerach jedynie z centralnej konsoli zarządzającej.	
136.	Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.	
137.	Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu min:	

Fundusze Europejskie
Program RegionalnyRzeczpospolita
Polska

Śląskie.

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego

	pdf, csv	
138.	Raport generowany według harmonogramu z możliwością automatycznego wysłania go do Osób zdefiniowanych w tym raporcie.	
139.	Możliwość dezinstalacji oprogramowania antywirusowego innych firm.	
140.	Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci lub z ustawieniami niestandardowymi.	
141.	Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.	
142.	Uwierzytelnianie dwuskładnikowe	
143.	Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji	

- Załącznik nr 7 – Część nr 2 – Dostawa komputerów przenośnych wraz z systemem operacyjnym – 10sztuk.

Poprzedni opis:

	Oprogramowanie antywirusowe	Nazwa/oznaczenie:
	Ochrona antywirusowa	
143.	Producent:	
144.	Typ/Model	
145.	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami	
146.	Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.	
147.	Wbudowana technologia do ochrony przed rootkitami.	
148.	Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	
149.	Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie”.	
150.	Skanowanie "na żądanie" pojedynczych plików lub katalogów	
151.	Możliwość skanowania dysków sieciowych i dysków przenośnych.	
152.	Możliwość umieszczenia na liście wykluczenia ze skanowania wybranych plików, katalogów lub plików o określonych	

	rozszerzeniach i procesów.	
153.	Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej za pomocą czytników (oprogramowania do obsługi poczty) email.	
154.	Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej] (niezależnie od konkretnego klienta pocztowego).	
155.	Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.	
156.	Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.	
157.	Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator.	
158.	Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.	
159.	Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.	
160.	Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora	
161.	Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń	
162.	Możliwość obsługi pobierania aktualizacji za pośrednictwem serwera proxy.	
163.	Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.	
164.	Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.	
165.	Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie urządzenie)	
166.	Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, z bazy danych urządzeń podłączanych przez użytkowników do komputerów.	
167.	Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.	
168.	Jedna wersja instalacyjna na stacje robocze i serwery plików.	
169.	Wbudowana zaporą osobista, umożliwiającą tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.	

Fundusze Europejskie
Program RegionalnyRzeczpospolita
Polska

Śląskie.

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego

170.	Możliwość tworzenia list sieci zaufanych.	
171.	Możliwość dezaktywacji funkcji zapory sieciowej	
172.	Hypervisor Introspection	
173.	Dla systemu Android możliwość blokowania stron internetowych.	
174.	Możliwość szyfrowania urządzenia opartego o system android.	
175.	Możliwość skanowania aplikacji w trakcie instalacji na urządzeniach z systemem Android	
	Oprogramowanie antywirusowe - Konsola zarządzająca	
176.	Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows, zdalna instalacja na środowiskach wirtualnych.	
177.	Możliwość integracji z kontem Domenowym Active Directory	
178.	Centralna konfiguracja i zarządzanie ochroną antywirusową antyspyware'ową oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych z jednego serwera zarządzającego.	
179.	Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.	
180.	Możliwość sprawdzenia z centralnej konsoli zarządzającej Stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).	
181.	Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.	
182.	Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.	
183.	Możliwość zmiany konfiguracji na stacjach i serwerach jedynie z centralnej konsoli zarządzającej.	
184.	Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.	
185.	Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu min: pdf, csv	

186.	Raport generowany według harmonogramu z możliwością automatycznego wysłania go do Osób zdefiniowanych w tym raporcie.	
187.	Możliwość dezinstalacji oprogramowania antywirusowego innych firm.	
188.	Tworzenie osobnych polityk dla fizycznych komputerów, urządzeń mobilnych oraz maszyn wirtualnych.	
189.	Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci lub z ustawieniami niestandardowymi.	
190.	Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.	
191.	Uwierzytelnianie dwuskładnikowe	
192.	Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji	

Zmodyfikowany Opis:

	Oprogramowanie antywirusowe	Nazwa/oznaczenie:
	Ochrona antywirusowa	
143.	Producent:	
144.	Typ/Model	
145.	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami	
146.	Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.	
147.	Wbudowana technologia do ochrony przed rootkitami.	
148.	Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	
149.	Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie”.	
150.	Skanowanie "na żądanie" pojedynczych plików lub katalogów	
151.	Możliwość skanowania dysków sieciowych i dysków przenośnych.	
152.	Możliwość umieszczenia na liście wykluczenia ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach i procesów.	

Fundusze Europejskie
Program RegionalnyRzeczpospolita
Polska

Śląskie.

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego

153.	Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej za pomocą czytników (oprogramowania do obsługi poczty) email.	
154.	Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej] (niezależnie od konkretnego klienta pocztowego).	
155.	Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.	
156.	Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.	
157.	Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator.	
158.	Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.	
159.	Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.	
160.	Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora	
161.	Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń	
162.	Możliwość obsługi pobierania aktualizacji za pośrednictwem serwera proxy.	
163.	Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.	
164.	Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.	
165.	Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie urządzenie)	
166.	Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, z bazy danych urządzeń podłączanych przez użytkowników do komputerów.	
167.	Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.	
168.	Jedna wersja instalacyjna na stacje robocze i serwery plików.	
169.	Wbudowana zaporą osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.	
170.	Możliwość tworzenia list sieci zaufanych.	



Fundusze Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



171.	Możliwość dezaktywacji funkcji zapory sieciowej	
	Oprogramowanie antywirusowe - Konsola zarządzająca	
172.	Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows, zdalna instalacja na środowiskach wirtualnych.	
173.	Możliwość integracji z kontem Domenowym Active Directory	
174.	Centralna konfiguracja i zarządzanie ochroną antywirusową antyspyware'ową oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych z jednego serwera zarządzającego.	
175.	Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.	
176.	Możliwość sprawdzenia z centralnej konsoli zarządzającej Stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).	
177.	Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.	
178.	Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.	
179.	Możliwość zmiany konfiguracji na stacjach i serwerach jedynie z centralnej konsoli zarządzającej.	
180.	Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.	
181.	Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu min: pdf, csv	
182.	Raport generowany według harmonogramu z możliwością automatycznego wysłania go do Osób zdefiniowanych w tym raporcie.	
183.	Możliwość dezinstalacji oprogramowania antywirusowego innych firm.	
184.	Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci lub z ustawieniami niestandardowymi.	
185.	Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.	
186.	Uwierzytelnianie dwuskładnikowe	



Fundusze
Europejskie
Program Regionalny



Rzeczpospolita
Polska



Śląskie.

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



187.	Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji	
------	--	--

Zamawiający informuje, iż zmodyfikowane załączniki stanowią integralną część SWZ.

W imieniu Zamawiającego

ZASTĘPCA DYREKTORA
ds. Administracyjno-Technicznych
Szpitala Specjalistycznego Nr 2 w Bytomiu
Wojciech Wiczorek