Załącznik nr 6 – Uszczegółowienie przedmiotu zamówienia

Tabela 1	
Oprogramowanie antywirusowe typu Bitdefender GravityZone Business Security lub równoważne	**Ilość licencji – 150 sztuk**
Lp.	**Kryteria równoważności (wymagania minimalne):**
1.	**W zakresie funkcjonalności**
1.1.	**Ochrona antywirusowa i antyspyware:** 1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim 3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 4. Wbudowana technologia do ochrony przed rootkitami. 5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 8. Możliwość skanowania dysków sieciowych i dysków przenośnych. 9. Skanowanie plików spakowanych i skompresowanych. 10. Możliwość umieszczenia na liście wykluczenia ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach i procesów. 11. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express. 12. 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). 13. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 14. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 15. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta. 16. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 17. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać. 18. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS. 19. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.

	20. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło. 21. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie" możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony. 22. Możliwość pobrania płyty ratunkowej, do uruchomienia z niej komputera i przeskanowania dysków umieszczonych w komputerze. 23. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 24. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB powinien pracować w trybie graficznym. 25. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 26. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 27. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej. 28. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet. 29. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej. 30. Możliwość odblokowania ustawień programu po wpisaniu hasła 31. Posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu modułu Super użytkownika 32. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie) 33. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, z bazy danych urządzeń podłączanych przez użytkowników do komputerów. 34. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp. 35. Funkcja Ochrony danych konfigurowana zdalnie przez administratora. 36. Jedna wersja instalacyjna na stacje robocze i serwery plików. 37. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego. 38. Wbudowany IDS 39. Możliwość zainstalowania silnika pełnego, lekkiego z sprawdzaniem reputacji plików w chmurze. 40. Możliwość tworzenia list sieci zaufanych. 41. Możliwość dezaktywacji funkcji zapory sieciowej. 42. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. 43. Dodatkowy moduł ochrony przeciwko zagrożeniom typu ransomware 44. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji 45. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań(konfigurowalne w politykach bezpieczeństwa) 46. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi 47. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups 48. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do

	serwera zarządzającego.
1.2.	**Maszyny Wirtualne:** 1. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu) 2. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej. 3. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem 4. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym. 5. Możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta. 6. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
1.3.	**Serwery Windows:** 1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 3. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 6. Skanowanie plików spakowanych i skompresowanych. 7. Oprogramowanie powinno zawierać monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego. 8. Oprogramowanie powinno posiadać możliwość zablokowania hasłem odinstalowania programu. 9. powinny być aktualizowane nie rzadziej niż raz na godzinę. 10. Oprogramowanie powinno posiadać możliwość raportowania zdarzeń informacyjnych. 11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju. 12. Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych plików. 13. Program musi mieć wbudowany skaner wyszukiwania rootkitów 14. Możliwość odblokowania ustawień programu po wpisaniu hasła 15. Możliwość uruchomienia zadania skanowania z niskim priorytetem
1.4.	**Konsola zdalnej administracji**

	1. Dwa typy konsoli administracyjnej: • Konsola Cloud – serwer administracyjny po stronie producenta • Konsola On-premise – lokalny serwer administracyjny 2. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows. 3. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego. 4. Możliwość integracji z kontem Domenowym Active Directory w obu rodzajach konsoli. 5. W Konsoli Cloud dostępna jest tylko jedna maszyna integrująca z domeną Active Directory. 6. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych. 7. 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). 8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego. 9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu. 10. Możliwość zmiany konfiguracji na stacjach i serwerach jedynie z centralnej konsoli zarządzającej. 11. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi 12. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej. 13. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv 14. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip. 15. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu. 16. Możliwość dezinstalacji oprogramowania antywirusowego innych firm. 17. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej. 18. Możliwość synchronizacji serwera administracyjnego z Active Directory (On Premis) 19. Wykorzystanie nie relacyjnej bazy danych MongoDB w serwerze zarzadzania. 20. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania. 21. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego. 22. Możliwość przypisywania polityk w zależności na jakim połączeniu użytkownik się znajduje (wifi, sieć przewodowa), DNS, IP, Brama itp. 23. Integracja z zewnętrznym serwerem Syslog 24. Integracja z ConnectWise 25. Uwierzytelnienie dwuskładnikowe
2.	**Obsługiwane systemy operacyjne**
2.1.	min.: - Windows 10 Anniversary Update "Redstone", - Windows 10 TH2, - Windows 10,

	- Windows 8.1, - Windows 8, - Windows 7, - Windows Server 2016, - Windows Server 2012 , - Windows Server 2012 R2, - Windows Server 2008 / Windows Server 2008 R2 -Red Hat Enterprise Linux / CentOS 5.6 lub wyższy - Ubuntu 12.04 lub wyższy - SUSE Linux Enterprise Server 11 lub wyższy - Debian 7.0 lub wyższy - Oracle Linux 6.3 lub nowszy
3.	**Wdrożenie**
3.3.	- Wykonawca zapewni zdalne wdrożenie wraz ze zdalnym szkoleniem z oprogramowania - Nabyta licencja powinna być aktywna od dnia 01.03.2019
4.	**Pomoc techniczna**
4.1	W ramach zakupionej licencji oprogramowania Zamawiający będzie miał zapewnioną zdalną, darmową pomoc techniczną inżyniera producenta przez cały okres trwania licencji