ZAŁĄCZNIK NR 1 do SWZ

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.
Zamawiający zaleca zapisanie dokumentu w formacie PDF.

Formularz asortymentowo – cenowy

PAKIET NR 1 - Dostawa licencji na oprogramowanie klasy Endpoint Detection and Response w architekturze serwera

Lp.	Przedmiot zamówienia	j.m.	Ilość	Cena netto za jednostkę miary w PLN	Stawka VAT (%)	Wartość brutto ogółem w PLN
1.	Dostawa licencji na oprogramowanie klasy Endpoint Detection and Response w architekturze serwera	komplet	1			

Oferowane oprogramowanie (podać typ i nazwę producenta):

Typ .....

Nazwa producenta .....

Zestawienie wymaganych parametrów technicznych

Przedmiot zamówienia obejmuje dostawę licencji na oprogramowanie klasy Endpoint Detection and Response w architekturze serwera wraz z usługą wsparcia przy wdrożeniu zgodnie z poniżej określonymi wymaganiami.

Lp.	Wymagane parametry techniczne (wartości minimalne wymagane)	Oferowane parametry
Wymagania ogólne		
1.	Zamawiający wymaga dostarczenia 250 licencji oprogramowania antywirusowego wraz z modułem EDR na okres 60 miesięcy o parametrach określonych w OPZ.	
2.	Zamawiający wymaga pomocy zdalnej przy wdrożeniu proponowanego rozwiązania przez certyfikowanego inżyniera tego rozwiązania.	
3.	Zamawiający wymaga aby oferent wraz z oprogramowaniem dostarczył cztery vouchery na szkolenia zdalne zorganizowane przez autoryzowany przez producenta ośrodek szkoleniowy. Szkolenie minimum trzy dniowe z obsługi konsoli centralnego zarządzania oraz modułu EDR.	
4.	Rozwiązanie musi posiadać wsparcie polskojęzyczne na okres minimum 60 miesięcy, obejmujące w szczególności: 1) Dostęp do poprawek i uaktualnień Oprogramowania 2) Dostęp do polskojęzycznego wsparcia drogą telefoniczną, mailową, bądź przez dedykowany portal. Wsparcie również obejmuje prawo do aktualizacji	
5.	Rozwiązanie musi wspierać systemy operacyjne Windows 7/8/8.1/10/11, przy czym najnowsza wersja systemu musi wspierać przynajmniej systemy Windows 10 oraz Windows 11.	
6.	Rozwiązanie musi zapewniać wsparcie dla 32- i 64-bitowej wersji systemu Windows.	
7.	Wersja systemu na stacjach roboczych Windows dostępna w języku polskim.	
8.	Wsparcie techniczne do systemu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta systemu.	
Wymagania w zakresie zarządzania zdalnego		
9.	1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server (od 2012) oraz na systemach Linux. 2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD. 3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL. 4. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. 5. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL. 6. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów. 7. Rozwiązanie musi zapewniać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. 8. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona	

	antywirusowa, antyspyware, które działają na stacjach roboczych w sieci. 9. Rozwiązanie musi zapewniać weryfikację 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). 10. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. 11. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 12. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory. 13. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 14. Grupy dynamiczne muszą być tworzone 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. 15. Rozwiązanie musi zapewniać korzystanie z minimum 80 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora. 16. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. 17. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.	
Wymagania w zakresie ochrony stacji roboczych		
10.	1. Rozwiązanie musi wspierać systemy operacyjne Windows 7/8/8.1/10/11. 2. Rozwiązanie musi wspierać architekturę ARM64. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji 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. 14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, 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. 17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które	

	z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 21. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego MS Outlook. 22. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: • tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, • tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. 23. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. 24. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 25. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 27. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 28. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 29. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.	
Wymagania w zakresie ochrony serwerów		
11.	1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux. 2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. **Dodatkowe wymagania dla ochrony serwerów Windows:** 9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji 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. 14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. **Dodatkowe wymagania dla ochrony serwerów Linux:** 18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 20. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.	
Wymagania w zakresie ochrony urządzeń mobilnych opartych o system Android		
12.	1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.	

	3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: a) nazwę aplikacji, b) nazwę pakietu, c) kategorię sklepu Google Play, d) uprawnienia aplikacji, e) pochodzenie aplikacji z nieznanego źródła.	
Szyfrowanie		
13.	1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit. 2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.	
Endpoint Detection and Response		
14.	1. Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS współpracujący z systemem do ochrony stacji roboczych tego samego producenta. 2. Rozwiązanie musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta. 3. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 4. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 5. Rozwiązanie musi zapewniać wykluczenia dotyczące procesu lub procesu „rodzica". 6. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia. 7. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 8. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 9. Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne, pobrania do analizy oraz ich zablokowania. 10. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.	

Kolumna „Oferowane parametry" musi być w całości wypełniona. Wykonawca zobowiązany jest do podania oferowanych parametrów w następujących jednostkach:

TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę

NIE – wykonawca nie spełnia konkretnego parametru

Wartości określone w kolumnie „Wymagane parametry techniczne (wartości minimalne wymagane)" należy traktować jako niezbędne minimum, którego niespełnienie będzie skutkowało odrzuceniem oferty.

PAKIET NR 2 - Dostawa systemu ochrony poczty zapewniającego kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową

Lp.	Przedmiot zamówienia	j.m.	Ilość	Cena netto za jednostkę miary w PLN	Stawka VAT (%)	Wartość brutto ogółem w PLN
1.	Dostawa systemu ochrony poczty zapewniającego kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową	komplet	1			

Oferowany system ochrony poczty (podać typ i nazwę producenta):

Typ .....

Nazwa producenta .....

Zestawienie wymaganych parametrów technicznych

Przedmiot zamówienia obejmuje dostawę systemu filtrowania poczty elektronicznej w postaci urządzenia wraz z usługą wsparcia przy wdrożeniu zgodnie z poniżej określonymi wymaganiami.

Lp.	Wymagane parametry techniczne (wartości minimalne wymagane)	Oferowane parametry
Wymagania ogólne		
1.	Zamawiający wymaga dostarczenia systemu filtrowania poczty elektronicznej w postaci urządzenia w OPZ.	
2.	Zamawiający wymaga, aby Wykonawca dostarczył rozwiązanie i wdrożył system ochrony poczty do infrastruktura Zamawiającego.	
3.	Zamawiający wymaga aby Wykonawca przeprowadził autoryzowane szkolenie w zakresie obsługi dostarczanego systemu dla czterech uczestników.	
4.	System ochrony poczty musi obejmować mechanizmy SPF, DMARC, DKIM, antyspam oraz ochronę antywirusową.	
Parametry techniczne		
5.	1. Obudowa typu RACK 19" o wysokości 1U. 2. Minimalna liczba interfejsów sieciowych urządzenia to co najmniej 1 interfejs Gigabit. 3. Urządzenie przeznaczone jest do obsługi min. 700 użytkowników. 4. Ilość przestrzeni dyskowej przeznaczonej na kwarantannę to minimum 20GB. 5. Liczba obsługiwanych domen: min. 20. 6. Przestrzeń dyskowa logów i bufora wiadomości: nie mniejsza niż 12 GB. 7. Kwarantanna działająca w trybie globalnym (adres email przeznaczony do odbioru wiadomości co do których podjęto decyzję o kwarantannie) z obsługą w logu wiadomości.	
Wymagania w zakresie ochrony przed spamem		
6.	1. Urządzenie ma: a) zapewniać ochronę zarówno poczty przychodzącej jak i wychodzącej, b) zapobiegać próbom spoofingu, phisingu i spyware, c) zabezpieczać przed atakami typu DoS (Denial of Service), d) zabezpieczać pocztę wychodzącą, w skład której wchodzi ochrona antywirusowa, kontrola ilości wysłanych wiadomości przez użytkownika, e) zapewniać ochronę przed atakami typu DHA (Directory Harvest Attack). 2. Możliwość ustawiania progów na podstawie punktacji przypisanej przez algorytmy modułu antyspamowego dla wiadomości przychodzących, wg której wiadomości mogą być blokowane, przesyłane do kwarantanny lub oznaczane jako spam. 3. Możliwość ustawiania progów na podstawie punktacji przypisanej przez algorytmy modułu antyspamowego dla wiadomości wychodzących, wg której wiadomości mogą być blokowane lub przesyłane do kwarantanny. 4. Analiza odcisku palca wiadomości (fingerprint), pozwalająca na zweryfikowanie wiadomości przychodzącej z bazą odcisków wiadomości zawierających spam, stworzonej przez producenta. 5. Analiza obrazów dołączonych do wiadomości przy pomocy skanera OCR (Optical Character Recognition). 6. Weryfikacja adresów URL zawartych w wiadomości z bazą danych znanych adresów URL zawierających spam. Możliwość blokowania, oznaczania, przenoszenia do kwarantanny takich wiadomości spamowych. 7. Urządzenie ma mieć możliwość korzystania z filtrów Bayesa. 8. Możliwość określania maksymalnej ilości połączeń z danego adresu IP do urządzenia, w zdefiniowanym przez administratora przedziale czasu. Ustawienie dotyczy zarówno poczty wychodzącej jak i przychodzącej. 9. Możliwość określania maksymalnej ilości wysłanych wiadomości od danego nadawcy w zdefiniowanym przez administratora przedziale czasu. Ustawienie dotyczy poczty wychodzącej. 10. Możliwość zdefiniowania adresów email wyłączonych ze sprawdzania maksymalnej ilości wysyłanych wiadomości w zdefiniowanym przez administratora przedziale czasu.	

	11. Możliwość zdefiniowania adresów email wyłączonych ze sprawdzania maksymalnej ilości wysyłanych wiadomości w zdefiniowanym przez administratora przedziale czasu. 12. Uwierzytelnianie nadawcy wiadomości na podstawie SPF (Sender Policy Framework). 13. Uwierzytelnianie nadawcy wiadomości na podstawie mechanizmu DKIM (Domain Keys). 14. Zapobieganie niepożądanym wiadomościom bounce z wykorzystaniem metody oznaczania nagłówków wiadomości wysyłanych przez urządzenie. 15. Możliwość korzystania z dowolnych zewnętrznych baz RBL. 16. Urządzenie ma zapewniać dostęp do baz reputacyjnych producenta, które zawierają listę znanych spamerów. 17. Możliwość zdefiniowania wykluczeń ze skanowania antyspamowego dla wiadomości wychodzących/przychodzących ze określonego adresu IP lub zakresu adresów IP. 18. Możliwość zdefiniowania akcji dla wiadomości przychodzących w przypadku gdy wiadomości zostały wysłane z określonego adresu IP lub określonej podsieci. Dostępne akcje w tym przypadku to: blokowanie, poddanie kwarantannie lub oznaczenie wiadomości jako spam. 19. Możliwość zdefiniowania białej listy domen, subdomen. 20. Możliwość zdefiniowania czarnej listy domen, subdomen. Wiadomości przychodzące z tych domen/subdomen mogą być blokowane, oznaczone jako spam lub przenoszone do kwarantanny. 21. Możliwość określenia dla jakich domen chronionych przez urządzenie poczta wychodząca będzie szyfrowana przy pomocy protokołu TLS. 22. Możliwość określenia domen chronionych przez urządzenie, dla których poczta wychodząca będzie przekierowana na inny serwer pocztowy. 23. Możliwość określenia dla jakich adresów email poczta wychodząca będzie szyfrowana przy pomocy protokołu TLS. 24. Możliwość określenia adresów email, dla których poczta wychodząca będzie przekierowana na inny serwer pocztowy. 25. Możliwość blokowania wiadomości pochodzących z konkretnego kraju. 26. Możliwość tworzenia reguł pozwalających na blokowanie, przesyłanie do kwarantanny lub oznaczenia wiadomości jako spam wiadomości pochodzących z danego hosta. 27. Produkt powinien rozróżniać co najmniej 11 różnych zestawów znaków, różnych narodowości używanych do kodowania wiadomości mailowych. Wiadomości posiadające takie znaki mogą być blokowane, przesłane do kwarantanny lub oznaczone jako spam. 28. Urządzenie ma umożliwiać korzystanie użytkownikom z dodatkowego pluginu do aplikacji Microsoft Outlook. 29. Możliwość uruchomienia SMTP over TLS zarówno dla połączeń wychodzących jak i przychodzących. 30. Możliwość wymuszenia zgodności protokołu SMTP z RFC 821. 31. Możliwość blokowania wiadomości które nie używają FQDN (fully-qualified domain name) w polu 'From' adresu.	
Wymagania w zakresie kontroli treści		
7.	1. Kontrola zawartości załączników po: a) typie pliku, co najmniej następujące typy: MS Access, MS Excel, MS Word, Adobe PDF, MS PowerPoint, Windows exe, Windows Script. Skaner sprawdza również archiwa pod kątem obecności zdefiniowanych typów pliku, b) nazwie pliku lub rozszerzenia pliku, definiowane przez administratora, c) typie MIME pliku, definiowane przez administratora zgodnie ze standardem RFC. 2. Dostępne akcje w przypadku kontroli załączników wiadomości mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą: a) poczta przychodząca: blokowanie, przeniesienie do kwarantanny, b) poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie, przekierowanie na inny serwer. 3. Dostępne akcje w przypadku spakowanych, zabezpieczonych hasłem załączników wiadomości mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą: a) poczta przychodząca: blokowanie, przeniesienie do kwarantanny, b) poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie, przekierowanie na inny serwer. 4. Możliwość tworzenia reguł, przy pomocy wyrażeń regularnych filtrujących wiadomości po temacie, nagłówku i treści wiadomości. Możliwość tworzenia takich reguł zarówno dla wiadomości przychodzącej jak i wychodzącej. Dostępne akcje mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą: a) poczta przychodząca: blokowanie, przeniesienie do kwarantanny, oznaczenie wiadomości, dodanie do białej listy, b) poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie wiadomości, dodanie do białej listy, przekierowanie na inny serwer. 5. Minimum 4 predefiniowane, stworzone przez producenta reguły poczty wychodzącej, filtrujące wiadomości po temacie, nagłówku i treści wiadomości.	
Wymagania w zakresie ochrony antywirusowej		
8.	1. Urządzenie ma zapewniać skanowanie antywirusowe poczty przychodzącej przy pomocy minimum 3 różnych silników antywirusowych działających jednocześnie. 2. Weryfikacja odcisku wiadomości lub wirusa z bazą danych producenta, jeżeli informacje na temat tej wiadomości lub wirusa nie zostały odnalezione w lokalnej bazie na urządzeniu.	
Administracja		
9.	1. Urządzenie ma posiadać możliwość przywrócenia poprzednich zainstalowanych wersji firmware: ma być możliwość przywrócenia do wcześniej zainstalowanej wersji firmware lub do wersji, która została zainstalowana fabrycznie. 2. Urządzenie ma mieć możliwość przywrócenia poprzednio zainstalowanej bazy sygnatur wirusów. 3. Urządzenie ma mieć możliwość przywrócenia poprzednio zainstalowanej bazy sygnatur antyspamowych.	

	4. Urządzenie ma być konfigurowane za pomocą graficznego interfejsu dostępnego przez przeglądarkę internetową. 5. Interfejs administratora ma być dostępny w języku polskim. 6. Możliwość określenia czy administratorzy mają dostęp do interfejsu dostępnego przez przeglądarkę tylko poprzez protokół https. 7. Urządzenie ma mieć możliwość integracji z usługami katalogowymi LDAP oraz Active Directory przynajmniej do weryfikacji docelowych odbiorców przychodzących przesyłek pocztowych. 8. Urządzenie ma mieć możliwość skonfigurowania wirtualnych adresów IP do fizycznej karty sieciowej urządzenia. 9. Urządzenie ma mieć możliwość konfigurowania tras statycznych. 10. Urządzenie ma mieć możliwość przeprowadzenia diagnostyki poprzez interfejs graficzny przy użyciu narzędzi takich jak: ping, telnet, dig, tcpdump, traceroute. 11. Urządzenie ma mieć możliwość uruchomienia bezpiecznego, szyfrowanego połączenia z działem wsparcia technicznego producenta na życzenie administratora. 12. Urządzenie ma mieć możliwość tworzenia kopii zapasowej konfiguracji urządzenia, ustawień wszystkich lub wybranych użytkowników. 13. Kopie zapasowe mają być tworzone na żądanie lub eksportowane zgodnie z harmonogramem na zdefiniowany serwer ftp i smb. 14. Możliwość określenia maksymalnej liczby plików kopii zapasowej przechowywanej na serwerze ftp i smb. 15. Możliwość tworzenia kopii zapasowej baz danych filtrów Bayesa, dla całego systemu lub dla poszczególnych użytkowników. 16. Możliwość skonfigurowania adresu email, na który będą przesyłane kopie każdej wiadomości przychodzącej lub wychodzącej z urządzenia.	
Raportowanie		
10.	System raportowania powinien być dostępny z poziomu przeglądarki: 1. Możliwość wyświetlenia natychmiastowych raportów 2. Możliwość zaplanowania raportów zgodnie z harmonogramem 3. Zestaw odstępnych raportów powinien obejmować co najmniej: nadawców spamu, odbiorców spamu, aktywność w rozsyłaniu wirusów, raport o nietypowych rozmiarach wiadomości, raport o naruszeniach protokołu SPF	
Licencje		
11.	Oferowane rozwiązanie musi posiadać minimum pięcioletnią licencję obejmującą aktualizacje mechanizmów bezpieczeństwa m.in.: a) Sygnatur antyspamu, b) Sygnatur wirusów, c) Bazy danych reputacji, d) Analizy fingerprint, e) Analizy intencji, f) Reguł spamu obrazkowego, g) Reguł spamu tradycyjnego. h) Ochrona przed zero-day, tzw. sandboxing	
Gwarancja		
12.	Minimum 60-miesięczna gwarancja producenta obejmująca wszystkie elementy urządzenia zapewniająca w przypadku awarii wysłanie sprawnego sprzętu na wymianę na następny dzień roboczy od momentu zgłoszenia do serwisu producenta. Wymagany poziom serwisu SLA 8x5xNBD Gwarancja musi zapewniać również dostęp do poprawek oprogramowania oraz wsparcia technicznego producenta. Po upływie 4 lat Zamawiający musi posiadać możliwość nieodpłatnej wymiany sprzętu na fabrycznie nowe urządzenie w aktualnej (na moment wymiany) wersji sprzętowej w ramach tej samej serii/linii produktowej. Dostarczone urządzenie musi być fabrycznie nowe, nieużywane w żadnych projektach, nie może być rekondycjonowane, powystawowe, nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy, musi pochodzić z autoryzowanego kanału sprzedaży producenta i być przeznaczone na rynek Unii Europejskiej (znak CE).	

Kolumna „Oferowane parametry" musi być w całości wypełniona. Wykonawca zobowiązany jest do podania oferowanych parametrów w następujących jednostkach:

TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę

NIE – wykonawca nie spełnia konkretnego parametru

Wartości określone w kolumnie „Wymagane parametry techniczne (wartości minimalne wymagane)" należy traktować jako niezbędne minimum, którego niespełnienie będzie skutkowało odrzuceniem oferty.