Załącznik do zapytania o wycenę

Szczegółowy opis przedmiotu zamówienia

1. **Opis środowiska i założenia:**
   1) Zamawiający posiada środowisko wirtualizacyjne oparte na oprogramowaniu VMware (vSphere7 Essentials Plus);
   2) Zamawiający w zakresie usługi pocztowej korzysta z oprogramowania Microsoft Office 365;
   3) Zamawiający planuje uruchomienie systemu ochrony poczty internetowej w prywatnej chmurze obliczeniowej (VMware). System ochrony poczty internetowej będzie pełnił funkcje bramki pomiędzy klientami, a serwerem pocztowym (Microsoft Office 365).
2. **Przedmiot zamówienia:**

   Przedmiotem zamówienia jest dostawa oprogramowania wraz z licencją umożliwiającą uruchomienie systemu ochrony poczty w chmurze obliczeniowej Zamawiającego (dalej jako: „System") i zapewnienie usługi wsparcia technicznego producenta Systemu.

Specyfikacja minimalnych wymagań dla Systemu:

Lp.	**Funkcje**	**Wymagania minimalne**
1.	Funkcje logowania i raportowania	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1) logowanie do zewnętrznego serwera SYSLOG; 2) logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku; 3) logowanie informacji na temat obsługiwanych przez system wiadomości, spamu oraz niedozwolonych załączników; 4) możliwość podglądu logów w czasie rzeczywistym; 5) powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych; 6) predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu; 7) możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu; 8) system musi przechowywać logi pełnej historii zdarzeń takich jak (ale nie ograniczonych do): logowanie i próby logowania, operacje na zasobach, modyfikacje uprawnień użytkowników, dodawanie grup i użytkowników, kasowanie obiektów.

2.	Ogólne funkcje systemu ochrony poczty	Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje: 1) wsparcie dla co najmniej 50 domen pocztowych; 2) polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all); 3) email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP; 4) zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości); 5) ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej; 6) szczegółowe, wielowarstwowe polityki wykrywania spamu oraz złośliwego oprogramowania; 7) możliwość tworzenia polityk kontroli antywirusowej oraz antyspamowej w oparciu użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP; 8) kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania wiadomości z kwarantanny przez użytkownika; 9) dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz POP3; 10) backup konfiguracji realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI; 11) białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu, funkcjonalność definiowania białych i czarnych list adresów mailowych dla poszczególnych użytkowników; 12) zapobieganie przed wyciekiem informacji poufnej DLP (Data Leak Prevention) pozwalające na czytanie metadanych w przesyłanych plikach, czytanie treści wiadomości (w tym też nagłówków) oraz wyzwalanie akcji takich jak zablokowanie (reject oraz discard) wiadomości, dodanie nagłówka do wiadomości, powiadomienie użytkownika, poddanie

		kwarantannie, zaszyfrowanie wiadomości, dodanie BCC (UDW); 13) wsparcie dla TLS (serwer – serwer) z kontrolą szyfrów i ich egzekwowaniem; 14) wsparcie dla geolokalizacji adresów IP i możliwość wykorzystania geolokalizacji w politykach (np. blokowanie konkretnego państwa); 15) integracja (poprzez API) z Microsoft Office 365 umożliwiająca skanowanie w czasie rzeczywistym skrzynek pocztowych; 16) System musi być zgodne z SMTP RFC; 17) obsługa DANE (DNS-based Authentication of Named Entities); 18) System musi umożliwiać na pracę w trybie Gateway lub Transparent.
3.	Kontrola antywirusowa	Dostarczony System ochrony poczty musi zapewniać: 1) skanowanie antywirusowe wiadomości SMTP; 2) kwarantannę dla zainfekowanych plików; 3) skanowanie załączników skompresowanych oraz archiwów zagnieżdżonych; 4) definiowanie komunikatów powiadomień w języku polskim; 5) blokowanie załączników w oparciu o typ pliku; 6) możliwość zdefiniowania nie mniej niż 50 polityk kontroli antywirusowej; 7) moduł kontroli antywirusowej musi mieć możliwość integracji mechanizmów ochrony antywirusowej z rozwiązaniami sandboxowymi w celu rozpoznawania nieznanych dotąd zagrożeń. System musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania oceny zagrożenia; 8) definiowanie różnych akcji dla poszczególnych metod wykrywania złośliwego oprogramowania dla wiadomości przychodzących jak i wychodzących. Powinny one obejmować co najmniej: tagowanie wiadomości, dodawanie nagłówka, dopisywanie ostrzeżenia w treści wiadomości, poddawanie kwarantannie, odrzucanie (discard oraz denny), dodanie BCC (UDW).

4.	Kontrola antyspamowa	System musi zapewniać poniższe funkcje i metody filtrowania spamu: 1) reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy reputacji producenta Systemu; 2) filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta Systemu; 3) szczegółowa kontrola nagłówka wiadomości; 4) analiza heurystyczna; 5) współpraca z zewnętrznymi serwerami RBL, SURBL; 6) filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen; 7) możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników; 8) wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF; 9) wykrywanie spamu w oparciu o mechanizm analizy behawioralnej analizującej podobieństwa między skanowanym emailem, a znanym spamem znajdującym się w bazie spamu dostarczonej przez producenta oferowanego Systemu; 10) wykrywanie spamu w oparciu o mechanizm analizy podszywania się (impersonalizacja) - ręczne i automatyczne wykrywanie podszywania się pod adres email/osobę; 11) kontrola w oparciu o Greylisting; 12) filtrowanie treści wiadomości i załączników; 13) kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości; 14) możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej dla całego systemu; 15) System musi realizować skanowanie antyspamowe z wydajnością minimum 50 tysięcy wiadomości na godzinę; 16) ochrona typu outbrake; 17) filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking);

		18) wsparcie dla SPF, DKIM, DMARC oraz ARC; 19) ochrona w oparciu o wyrażenia regularne i zdefiniowany przez administratora słownik wyrazów; 20) definiowanie różnych akcji dla poszczególnych metod wykrywania spamu dla wiadomości przychodzących jak i wychodzących. Powinny one obejmować co najmniej: tagowanie wiadomości, dodawanie nagłówka, dopisywanie ostrzeżenia w treści wiadomości, poddawanie kwarantannie, odrzucanie (discard oraz denny), dodanie BCC (UDW).
5.	Ochrona treści	System musi zapewniać poniższe funkcje i metody ochrony treści: 1) wykrywanie aktywnej zawartości w plikach PDF i dokumentach Office; 2) neutralizacja dokumentów Office i PDF (usuwanie makr, aktywnej zawartości, załączników i innych); 3) ponowne skanowanie w poszukiwaniu zagrożeń przy zwolnieniu z kwarantanny; 4) wykrywanie MIME i typów plików; 5) tworzenie własnych filtrów plików; 6) odszyfrowywanie archiwów, plików PDF i dokumentów przy użyciu wbudowanych i zdefiniowanych przez administratora list haseł; 7) filtrowanie adresów URL z możliwością tworzenia swoich własnych kategorii adresów, które mają być filtrowane. Baza adresów URL powinna być dostarczona przez producenta oferowanego Systemu. 8) neutralizacja treści HTML wiadomości e-mail poprzez usunięcie hiperłączy / przepisanie adresów URL; 9) ochrona hiperłączy poprzez nadpisanie URL i przekierowanie do portalu weryfikującego „kliknięty” link; 10) wsparcie dla S/MIME; 11) automatyczne i bezagentowe szyfrowanie wiadomości na podstawie wybranych przez administratora atrybutów, takich jak treść tematu, treść wiadomości lub domena odbiorcy w trybie „Push” i „Pull”.
6.	Ochrona przed atakami na usługę	System musi zapewniać poniższe funkcje i metody filtrowania:

	poczty	1) ochrona przed atakami na adres odbiorcy; 2) ograniczenie liczby połączeń, jednoczesnych połączeń; 3) definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu; 4) kontrola Reverse DNS (ochrona przed Anty-Spoofing); 5) weryfikacja poprawności adresu e-mail nadawcy; 6) ochrona przed BEC (Business Email Compromise) tj. atakami phishingowymi lub socjotechnicznymi, których celem jest przede wszystkim kadra kierownicza wyższego szczebla oraz pracownicy działów finansowych.
7.	Funkcje pracy w trybie wysokiej dostępności (HA)	System ochrony poczty musi zapewniać poniższe funkcje: 1) konfigurację HA w każdym z trybów: gateway, transparent; 2) tryb A-P [Active-Passive] z synchronizacją polityk i wiadomości, gdzie klaster występuje pod jednym adresem IP; 3) tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP; 4) wykrywanie awarii poszczególnych elementów oraz powiadamianie administratora systemu; 5) monitorowanie stanu pracy klastra.
8.	Aktualizacje sygnatur, dostęp do bazy spamu	System ochrony poczty musi zapewniać: 1) pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym, 2) planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
9.	Zarządzanie	System ochrony poczty musi zapewniać poniższe funkcje: 1) możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH; 2) możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy; 3) wsparcie dla SAML 2.0 SSO i ADFS; 4) obsługa SNMP przy użyciu standardowej i prywatnych MIB z pułapkami opartymi na progach; 5) możliwość tworzenia kont administratora przypisywanych do konkretnych domen obsługiwanych przez System;

10.	Wsparcie producenta	1) wsparcie techniczne producenta Systemu na okres 24/36 miesięcy, od dnia dostawy Systemu; 2) wsparcia techniczne obejmuje nieograniczony dostęp do wszystkich udostępnionych przez producenta Systemu aktualizacji, poprawek, subskrypcji, baz sygnatur, dokumentacji technicznej, baz wiedzy oraz instrumentów do obsługi zgłoszeń serwisowych realizowanych przez producenta Systemu; 3) dostęp do uaktualnień sygnatur, poprawek i aktualizacji Systemu będzie realizowany przez konto udostępnione przez producenta wraz z niezbędnymi danymi logowania, umożliwiającymi samodzielne (bezpośrednio u producenta) pobieranie uaktualnień sygnatur/reguł oraz poprawek i aktualizacji w ramach posiadanej licencji oraz umożliwiającymi zakładanie zgłoszeń serwisowych 24 h przez 7 dni w tygodniu; 4) wsparcie producenta realizowane zdalnie, z czasem reakcji w zależności od poziomu krytyczności awarii/błędu od 60 minut do 24 godzin od przyjęcia zgłoszenia (szczegóły niżej), możliwość zgłaszania awarii poprzez dedykowany i zabezpieczony kanał komunikacji elektronicznej; 5) wsparcie producenta realizowane w trybie 8x5 24h Remote Response Time (dla niekrytycznego poziomu błędu/awarii) oraz 24x7x365 1h Remote Response Time (w przypadku krytycznego poziomu błędu/awarii); 6) szczegółowe warunki wsparcia technicznego dla Systemu, o którym mowa powyżej regulować powinny umowy licencyjne lub inne stosowne umowy lub warunki wydane lub zaakceptowane przez producenta Systemu, przy czym umowy takie, ani warunki nie mogą ograniczać wskazanych powyżej wymagań, ani stać z nimi w sprzeczności.
11.	Licencja	Licencja na jedną maszynę wirtualną.