Załącznik nr 2

Opis Przedmiotu zamówienia

OpenText Secure Messaging Gateway **(1 rok)**	511	01.01.2025 - 31.12.2025

Funkcje OpenText Secure Messaging Gateway na okres 1 roku lub równoważne:

1. **Filtracja treści**: Skuteczne filtrowanie wiadomości e-mail pod kątem niepożądanych treści, takich jak spam, phishing i złośliwe oprogramowanie.
2. **Skanowanie antywirusowe**: Posiada wbudowane narzędzia antywirusowe do wykrywania i usuwania wirusów oraz innego złośliwego oprogramowania w przychodzących i wychodzących wiadomościach.
3. **Ochrona przed phishingiem**: System musi posiadać zabezpieczenia chroniące przed próbami wyłudzenia danych poprzez identyfikację i blokowanie wiadomości phishingowych.
4. **Kontrola polityk bezpieczeństwa**: System musi mieć możliwość definiowania reguł i polityk dotyczących ruchu e-mailowego, np. blokowanie określonych typów załączników lub słów kluczowych.
5. **Szyfrowanie wiadomości**: System posiada opcje szyfrowania wiadomości e-mail, aby zapewniały bezpieczeństwo przesyłanych informacji i ochronę prywatności użytkowników.
6. **Obsługa zgodności (compliance)**: Posiada funkcje wspierające zgodność z wymaganiami prawnymi, takimi jak RODO, dzięki archiwizacji wiadomości i możliwości audytów.
7. **Raportowanie i analiza**: Posiada narzędzia do tworzenia raportów i monitorowania ruchu pocztowego, w tym alerty i statystyki dotyczące blokowanych zagrożeń.
8. **Ochrona przed wyciekiem danych (DLP)**: System ma mechanizmy zapobiegające wyciekowi poufnych informacji przez monitorowanie i blokowanie wrażliwych danych w e-mailach.
9. **Integracja z innymi systemami**: System ma możliwość integracji z innymi rozwiązaniami zabezpieczeń, serwerami pocztowymi oraz systemami zarządzania.
10. **Obsługa mechanizmów ochrony SPF, DKIM i DMARC**: system musi mieć możliwość weryfikacji sygnatur DKIM nadawcy i podpisywanie przesyłek wychodzących sygnaturą DKIM
11. **Integracja z GroupWise WEB**: skanowanie załączanych do przesyłek plików

12. **Zaawansowane filtrowanie antyspamowe**: System musi posiadać wielowarstwowe mechanizmy filtrowania spamu, które analizują nagłówki, treści i metadane wiadomości. Umożliwia blokowanie niechcianych wiadomości przy użyciu algorytmów sztucznej inteligencji i technik uczenia maszynowego, co minimalizuje liczbę fałszywych alarmów i zwiększa dokładność filtrowania.
13. **Adaptacyjne filtrowanie treści**: System musi analizować zawartość wiadomości pod kątem określonych fraz, wyrażeń oraz wzorców, pozwalając na dostosowywanie polityk bezpieczeństwa do potrzeb organizacji aby można było ograniczyć lub blokować treści uznane za nieodpowiednie, np. słowa kluczowe związane z niepożądanymi materiałami.
14. **Wielowarstwowe skanowanie antywirusowe**: System musi integrować się z popularnymi silnikami antywirusowymi i korzystać z nich, aby dokładnie skanować załączniki i treści wiadomości pod kątem złośliwego oprogramowania, wirusów, trojanów czy ransomware. Mechanizm ten musi wykrywać również zagrożenia typu zero-day i stosować aktualizacje w czasie rzeczywistym, aby maksymalizować ochronę przed nowymi zagrożeniami.
15. **Skanowanie linków (URL scanning)**: system musi skanować linki zawarte w wiadomościach i sprawdzać je pod kątem obecności złośliwych lub phishingowych stron

internetowych. Dzięki temu użytkownicy muszą być chronieni przed atakami phishingowymi, które mogą wyłudzać dane logowania lub inne poufne informacje.

16. **Szyfrowanie wiadomości i bezpieczna komunikacja**: System musi posiadać opcje szyfrowania wiadomości wychodzących, co umożliwia przesyłanie wrażliwych danych w sposób bezpieczny i zgodny z przepisami dotyczącymi ochrony danych, takimi jak RODO czy HIPAA. Wiadomości można szyfrować automatycznie na podstawie ustalonych reguł lub ręcznie.
17. **Funkcje DLP (Data Loss Prevention)**: system musi posiadać zaawansowane narzędzia DLP, które monitorują i zapobiegają wysyłaniu wiadomości zawierających dane poufne, np. numery kart kredytowych, dane osobowe czy inne wrażliwe informacje. Mechanizmy te mogą automatycznie blokować, szyfrować lub przekierowywać wiadomości, aby zapobiec nieuprawnionemu dostępowi.
18. **Automatyczne raportowanie i powiadomienia**: System musi umożliwiać generowanie szczegółowych raportów dotyczących ruchu pocztowego, blokowanych zagrożeń, poziomu spamu i aktywności użytkowników. Raporty te mogą być wysyłane automatycznie do administratorów, umożliwiając szybkie reagowanie na zagrożenia i monitorowanie skuteczności polityk bezpieczeństwa.
19. **Audyt i zgodność z przepisami**: system musi wspierać zgodność z przepisami poprzez archiwizację wiadomości, co umożliwia ich przegląd w razie audytów lub sporów prawnych. Przechowywane wiadomości można przeszukiwać, co wspiera transparentność i dostępność informacji.
20. **Polityki dostosowane do potrzeb organizacji**: Administratorzy mogą definiować szczegółowe polityki bezpieczeństwa, które dostosowują ochronę do wymogów urzędu, działu lub poszczególnych użytkowników. Możliwe jest ograniczenie dostępu do określonych załączników lub blokowanie konkretnych typów plików, co dodatkowo chroni infrastrukturę.
21. **Integracja z infrastrukturą IT**: system musi być kompatybilny z popularnymi systemami e-mail, takimi jak Microsoft Exchange, Office 365, Gmail czy serwery SMTP. Dzięki temu można go łatwo zintegrować z istniejącą infrastrukturą IT, co pozwala na centralne zarządzanie bezpieczeństwem poczty i utrzymanie spójności polityk.
22. **Monitorowanie w czasie rzeczywistym**: System musi oferować możliwość monitorowania aktywności i zagrożeń w czasie rzeczywistym. Administratorzy mogą otrzymywać natychmiastowe alerty o nietypowych aktywnościach, np. zwiększonym ruchu spamu lub wykryciu nowego wirusa, co pozwala na szybką reakcję.
23. **Moduł analizy i AI**: system musi korzystać z algorytmów sztucznej inteligencji do analizy wzorców ruchu i podejrzanych zachowań, co umożliwia szybsze wykrywanie anomalii oraz adaptacyjne dopasowywanie się do zmieniających się zagrożeń.