Dostawa z wdrożeniem oprogramowania zapewniającego kompleksowy monitoring infrastruktury IT oraz oprogramowania stacji roboczych PC Zamawiającego

1. Przedmiotem zamówienia jest dostawa z wdrożeniem oprogramowania zapewniającego kompleksowy monitoring infrastruktury IT oraz stanowisk użytkowników oprogramowania Zamawiającego.

2. Wykaz funkcjonalności w poszczególnych obszarach funkcjonalności oprogramowania:

2.1. Oprogramowanie musi pozwalać na monitorowane stacji roboczych opartych o systemy Windows, Linux oraz Mac.

2.2. Monitorowanie powinno być dostępne również dla urządzeń typu: firewall, router, przełącznik, VoIP, jak również drukarek pracujących w środowisku sieciowym oraz urządzeń obsługującychSNMP.

2.3. Serwer oprogramowania powinien działać w 64-bitowym systemie operacyjnym min. Windows Serwer 2019 oferującym 2 rdzenie CPU, 4GB RAM.

2.4. Konsole zarządzania powinny pracować w 64-bitowym systemie operacyjnym Microsoft Windows w konfiguracji 2 rdzenie CPU / 4 GB RAM

2.5. Minimalne wymagania dla agenta na stacjach roboczych nie powinny wykraczać poza 2 rdzeniowy CPU, 1GB RAM, i 32/64 bitowy system operacyjny Windows XP

2.6. Oprogramowanie Agenta powinno współpracować z posiadanymi rozwiązaniami bezpieczeństwa firmy Eset.

2.7. Monitorowanie infrastruktury IT z uwzględnieniem stacji roboczych, serwerów, sieciowych urządzeń aktywnych, urządzeń SNMP.
2.7.1. System powinien wykrywać urządzenia w sieci poprzez skanowanie ping oraz arp-ping.

2.7.2. Wykrywanie urządzeń na podstawie informacji odczytanych z AD.

2.7.3. Graficzna wizualizacja stanu urządzeń.

2.7.4. Wizualizacji poprzez tworzenie map i schematów dla urządzeń i połączeń.

2.7.5. Monitorowanie serwisów TCP/IP, HTTP, POP3, SMTP, FTP wraz z możliwością definiowania własnych rodzajów.

2.7.6. Monitorowanie czasu odpowiedzi i procent utraconych pakietów

2.7.7. Monitorowanie serwerów pocztowych ze szczególnym uwzględnieniem:
2.7.7.1. czas logowania,

2.7.7.2. czas wysyłania,

2.7.7.3. stanu powiadomienia (e-mail, SMS i inne),

2.7.7.4. wykonywania operacji testowych,
2.7.8. Monitorowanie serwerów WWW i adresów URL.

2.7.9. Monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS.

2.7.10. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail.

2.7.11. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją:

2.7.12. Obsługa komunikatów syslog i pułapek SNMP i ewidencjonowanie logów.

2.7.13. Monitoring aktywnego sprzętu sieciowego (firewalle, routery, przełączniki) w zakresie:
2.7.13.1. zmian stanu interfejsów sieciowych,

2.7.13.2. ruchu sieciowego,

2.7.13.3. podłączonych stacji roboczych z graficzną prezentacją przełącznika,

2.7.13.4. ruchu generowanego przez podłączone do portów stacje robocze
2.7.14. Monitorowanie serwisów Windows.

2.7.15. Wyświetlania statystyk urządzenia.

2.7.16. Monitorowanie wydajności systemów Windows

2.8. Inwentaryzacja zasobów IT w czasie rzeczywistym w zakresie fizycznym i logicznym.
2.8.1. Prezentacja pełnej specyfikacji komputera/stacji roboczej.

2.8.2. Zestawienie konfiguracji sprzętowej.

2.8.3. Powiadamianie o niezbędnej aktualizacji/rozszerzenia urządzenia.

2.8.4. Zestawienie zainstalowanych aplikacjach oraz aktualizacjach systemu operacyjnego.

2.8.5. Agregacja informacji o zmianach przeprowadzonych na wybranej stacji roboczej.

2.8.6. Możliwość wysyłania powiadomienia w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera

2.8.7. Możliwość odczytania numeru seryjnego (klucza licencyjnego).

2.8.8. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.

2.8.9. Możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań.

2.8.10. Możliwość tworzenia listy plików użytkowników z określonym rozszerzeniem znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).

2.8.11. Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików.

2.8.12. Możliwość przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji.

2.8.13. Tworzenia powiązań między zasobami a urządzeniami.

2.8.14. Tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z domeną AD).

2.8.15. Wskazania osób uprawnionych do użycia zasobów.

2.8.16. Możliwość definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania

dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz.

2.8.17. Możliwość określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów.

2.8.18. Możliwość określenia atrybutów dodatkowych tylko dla wybranych typów zasobów.

2.8.19. Możliwość definiowania własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie.

2.8.20. Możliwość importu danych z zewnętrznego źródła.

2.8.21. Możliwość przechowywania dowolnych dokumentów w postaci załączników.

2.8.22. Możliwość tworzenia powiązań między zasobami a dokumentami w relacji 1:N.

2.8.23. Możliwość oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,

2.8.24. Ewidencja czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności.

2.8.25. Generowanie zestawień wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania.

2.8.26. Generowanie protokołów przekazania zasobów.

2.8.27. Archiwizacja i porównywania audytów zasobów.

2.8.28. Tworzenia i drukowanie kodów dla zasobów które posiadają numer inwentarzowy.

2.8.29. Definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

2.8.30. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP

2.8.31. Prezentacja informacji o aplikacjach używanych w organizacji.

2.8.32. Tworzenie własnych wzorców aplikacji.

2.8.33. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.

2.8.34. Informacje o komputerach, na których aplikacja została wykryta.

2.8.35. Zarządzanie posiadanymi licencjami.

2.8.36. Wskazywanie osób odpowiedzialnych za licencję.

2.8.37. Wskazanie użytkowników licencji.

2.8.38. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.

2.8.39. Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.

2.8.40. Audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji.

2.8.41. Zarządzanie posiadanymi licencjami: raport zgodności licencji.

2.8.42. Możliwość przypisania do programów numerów seryjnych, wartości.
Możliwość instalacji zdalnej programów na stacjach roboczych zarówno na pojedynczym PC jak również grupie komputerów. Możliwość instalacji zdalnej programów dla pojedynczego konta AD oraz dla grupy kont AD.

2.9. Monitorowanie aktywności użytkowników systemu informatycznego.
2.9.1. Monitorowanie czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy)

2.9.2. Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach.

2.9.3. Monitorowanie rzeczywistego użytkowania programów.

2.9.4. Monitorowanie listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt).

2.9.5. Monitorowanie transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika).

2.9.6. Monitorowanie zleceń wydruków.

2.9.7. Monitorowanie nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

2.9.8. Możliwość blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest
użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.

2.9.9. Możliwość blokowania ruchu na wskazanych portach TCP/IP.

2.9.10. Możliwość blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem.

2.9.11. Wysyłanie powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia.

2.9.12. Definiowanie zakresu czasu w których monitorowanie użytkowników jest wyłączone.

2.10. Obsługa wewnętrznego Help Desk – zdalnej pomocy użytkownikom systemu informatycznego.
2.10.1. Możliwość prowadzenia kontroli stacji roboczej użytkownika z dostępem do pulpitu i zdalnego dostępu (w tym z dostępem bez zgody użytkownika i opcja, kiedy użytkownik decyduje o udzieleniu dostępu).

2.10.2. Obsługa funkcji zdalnego dostępu do stacji roboczej przez użytkownika, który uzyskał takie uprawnienia przez administratora systemu.

2.10.3. Pobieranie listy użytkowników z Active Directory.

2.10.4. Zarządzanie lokalnymi kontami Windows.

2.10.5. Zarządzanie dostępem pracowników Help Desk do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń.

2.10.6. Zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej.

2.10.7. Tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO.

2.10.8. Automatyczne przypisywanie pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników.

2.10.9. Procesowanie zgłoszeń użytkowników z wiadomości e-mail

2.10.10. Tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń.

2.10.11. Wykonywanie operacji na wielu zgłoszeniach równocześnie.

2.10.12. Dołączanie załączników do zgłoszeń.

2.10.13. Wyszukiwanie zgłoszeń i artykułów w bazie wiedzy.

2.10.14. Szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia.

2.10.15. Zrzuty ekranowe (podgląd pulpitu).

2.10.16. Dystrybucja oprogramowania przez funkcjonalność agenta

2.10.17. Dystrybucja oraz uruchamianie plików za pomocą Agentów (w tym plików MSI).

2.10.18. Zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku.

2.10.19. Możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami wysyłanymi do określonych aktorów w zgłoszeniu.

2.10.20. Obsługa usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem

2.10.21. Generowanie raportów obsługi helpdesk.

2.10.22. Zdalne wykonywanie poleceń poprzez agenta (np. utworzenie / edycja konta lokalnego użytkownika systemu).

2.10.23. Zarządzania procesami systemu Windows.

2.10.24. Wymiany plików do i ze stacji roboczej poprzez funkcję menedżera plików.

2.11. Ochrona danych przed nieuprawnionym dostępem do danych.

2.11.1. Możliwość blokowanie urządzeń i nośników danych.

2.11.2. Możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny

2.11.3. Blokowanie urządzeń i interfejsów fizycznych: USB, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD.

2.11.4. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth.

2.11.5. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.

2.11.6. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.

2.11.7. Funkcje wspierające bezpieczeństwa systemu: integracja i zarządzanie ustawieniami np. Windows Defender.

2.11.8. Funkcje wspierające bezpieczeństwo systemu:

2.11.9. Monitorowanie stanu szyfrowania dysków BitLocker.

2.11.10. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

2.11.11. Zarządzanie prawami dostępu do urządzeń:

2.11.11.1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.

2.11.11.2. Autoryzowanie urządzeń firmowych

2.11.11.3. Blokowanie urządzeń prywatnych

2.11.11.4. Blokowanie określonych typów urządzeń dla wybranych użytkowników.

2.11.11.5. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.

2.11.11.6. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

2.11.12. Audyt operacji na plikach na urządzeniach przenośnych:

2.11.12.1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.

2.11.12.2. Podłączenie/odłączenie urządzenia przenośnego.

2.11.13. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.

2.11.14. Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.

3. Wymagania w zakresie licencji i integracji:

3.1. Wieczysta licencja na oprogramowanie.

3.2. Podstawowy moduł zarządzania środowiskiem dla nielimitowanej liczby monitorowanych urządzeń.

3.3. Instalacja wielu zdalnych konsol administracyjnych w środowisku udostępnionym przez Zamawiającego – spełniającym wymogi oprogramowania Wykonawcy.

3.4. Umowa serwisowa obejmująca aktualizacje i pomoc techniczną na okres nie krótszy niż 36 miesięcy.

3.5. Modułowość oprogramowania pozwalająca Zamawiającemu na dowolną konfigurację według aktualnych potrzeb.

3.6. Obsługa 500 stacji roboczych przez wszystkie moduły i funkcjonalności oprogramowania z możliwością zwiększenia tej liczby w dowolnym czasie.

4. Wymagania w zakresie szkolenia personelu:

4.1. Zamawiający wymaga przeszkolenia w zakresie obsługi i administracji 4 osoby – administratorów systemu.

4.2. Szkolenia muszą mieć charakter ekspercki.

5. Warunki udzielenia licencji:

5.1. Licencje na oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej: klucze lub licencje dostępne do pobrania na stronie www producenta oprogramowania.

5.2. W przypadku licencji dostępnych w formie elektronicznej na stronie producenta, Wykonawca przekaże dane autoryzacyjne lub Zamawiający poda konto do portalu producenta, jakie posiada, a do którego licencje maja być dołączone.