

OPIS PRZEDMIOTU ANALIZY

Przedmiotem postępowania jest zakup wsparcia do posiadanych licencji na ochronę stacji roboczych albo dostawa oprogramowania równoważnego oraz wsparcia do posiadanych licencji służących do ochrony urządzeń mobilnych wraz z centralną konsolą zarządzającą albo dostawa oprogramowania równoważnego. Postępowanie zostało podzielone na dwie części.

Oferenci mogą składać oferty osobno do poszczególnych części.

CZĘŚĆ I – OCHRONA STACJI ROBOCZYCH

Przedmiotem zamówienia w części I jest odnowienie wsparcia producenta do posiadanych licencji systemu bezpieczeństwa albo dostawa oprogramowania równoważnego.

W chwili obecnej Zamawiający posiada wymienione w tabeli nr 1 licencje firmy SYMANTEC.

W ramach niniejszego zamówienia, Zamawiający wymaga przedłużenia wsparcia producenta do posiadanych licencji w okresie od dnia 2 sierpnia 2026 r. do dnia 1 sierpnia 2027 r.

Dostarczone przez Wykonawcę wsparcie producenta ma umożliwić bezpłatne wykonanie aktualizacji posiadanych licencji, do najnowszej wersji oprogramowania.

Tabela 1- Tabela dot. specyfikacji Symantec Endpoint Protection

Lp.	Opis produktu	Identyfikator Licencji	Ilość licencji
1	Symantec Endpoint Protection (aktualnie najnowsza wersja produktu)	Contract number: 52328117 Support Site ID: 375293 SKU: SUPPORT-SYMC4/SEP-PER	1500

W wypadku zaoferowania oprogramowania równoważnego oferent odpowiedzialny jest za:

- migracje całego środowiska do zaoferowanego oprogramowania,
- migracji polityk (antywirusowych, wykluczeń, polityk zapory ogniowej, polityk kontroli aplikacji i urządzeń),
- przeprowadzenie szkoleń dla administratorów systemu w zakresie używania nowego systemu, jaki i w zakresie przeprowadzonej implementacji.

Implementacja musi zostać udokumentowana dokumentem po wdrożeniowym zawierającym:

- implementacje,
- procedury odzyskiwania całego środowiska.

Tabela 1.1- Tabela dot. specyfikacji rozwiązania równoważnego

LP	Minimalne wymagania dla oprogramowania równoważnego dla pozycji 1 z Tabeli nr. 1: producent i nazwa produktu: uzupełnia Wykonawca ilość: uzupełnia Wykonawca	Deklaracja zgodności z opisem wymagań minimalnych Wstawić znak „X” we właściwą kratkę.
Ochrona antywirusowa:		
1.	Usuwanie wirusów, makro-wirusów, robaków internetowych oraz koni trojańskich (oraz wirusów i robaków z plików skompresowanych oraz samorozpakowujących się) lub kasowanie zainfekowanych plików. Ochrona	<input type="checkbox"/> Tak <input type="checkbox"/> Nie

	przed oprogramowaniem typu „spyware” i „adware”, włącznie z usuwaniem zmian wprowadzonych do systemu przez to oprogramowanie tego typu.	
2.	Wykrywanie wirusów, makro-wirusów, robaków internetowych, koni trojańskich, spyware, adware i dialerów ma być realizowane w pojedynczym systemie skanującym.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Określanie obciążenia CPU dla zadań skanowania zaplanowanego oraz skanowania na żądanie,	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
4.	Skanowanie zaplanowane musi umożliwiać automatyczne pomijanie plików uznanych przez producenta za zaufane	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
5.	Skanowanie plików pobranych z Internetu wraz ze skryptami umieszczonymi w sieci Internet oraz plików skompresowanych,	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
6.	Skanowanie plików pobranych z Internetu wraz ze skryptami umieszczonymi w sieci Internet oraz plików skompresowanych,	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
7.	<p>Zapewnienie stałej ochrony wszystkich zapisywanych, odczytywanych, a także uruchamianych plików przez mechanizm skanujący pracujący w tle wraz z metodą heurystyczną wyszukiwania wirusów (na życzenie); pliki te mogą być skanowane:</p> <ul style="list-style-type: none"> • na dyskach twardych • w boot sektorach • na dyskietkach • na płytach CD/DVD • na zewnętrznych dyskach twardych (np. podłączonych przez port USB) 	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
8.	Możliwość samodzielnego pobierania aktualizacji z Internetu do stacji roboczej	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
9.	Możliwość zablokowania funkcji zmiany konfiguracji klienta lub ukrycie interfejsu użytkownika klienta.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
10.	Scentralizowaną obsługę wirusów polegającą na przekazywaniu nieodwracalnie zainfekowanych plików do bezpiecznego miejsca w postaci centralnej kwarantanny na centralnym serwerze, w celu przeprowadzenia dalszych badań	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
11.	Wbudowana w oprogramowanie funkcja do wysyłania podejrzanych lub zainfekowanych nowymi wirusami plików do producenta w celu uzyskania szczepionek	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
12.	Wyszukiwanie i usuwanie wirusów w plikach skompresowanych (także zagnieżdżonych wewnątrz innych plików skompresowanych) w szczególności z plików typu ZIP, GNU, LZH/LHA, BinHex, ARJ, RAR, MIME/UU, TAR, kontenery CAB, UUE, Rich Text Format,	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
13.	Aktualizacja definicji wirusów nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie – serwerze czy stacji roboczej	<input type="checkbox"/> Tak <input type="checkbox"/> Nie

14.	Mikrodefinicje wirusów - przyrostowe, scentralizowane aktualizowanie klientów jedynie o nowe definicje wirusów i mechanizmy skanujące	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
15.	Możliwość cofnięcia procesu aktualizacji definicji wirusów i mechanizmów skanujących – powrót do poprzedniego zestawu definicji wirusów bez konieczności deinstalacji oprogramowania czy też restartu komputerów	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
16.	Możliwość natychmiastowego wymuszenia aktualizacji definicji wirusów na stacjach klienckich i serwerach.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
17.	Aktualizacja bazy definicji wirusów oraz mechanizmów skanujących, co najmniej 3 razy dziennie	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
18.	Aktualizacja baz definicji musi być aplikowana tylko w czasie nieaktywności użytkownika na komputerze – jeżeli użytkownik komputera na nim pracuje, aplikacja automatycznie zostaje opóźniona.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
19.	Możliwość aktualizacji bazy definicji wirusów średnio, co 1 godzinę	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
20.	Heurystyczna technologia do wykrywania nowych, nieznanых wirusów	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
21.	Dedykowany moduł analizy w czasie rzeczywistym zachowań aplikacji do wykrywania nowych, nieznanых zagrożeń typu robak internetowy, koń trojański, keylogger – analiza zachowania opiera się na wykonywanych przez aplikację czynnościach (tworzenie nowych plików, komunikacja z Internetem, podmiana strony w przeglądarce, itp.). Schematy szkodliwego działania powinny być generowane w procesie uczenia maszynowego (Machine Learning) zaimplementowanego na sieci składającej się z co najmniej 150milionów sond.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
22.	Dedykowany moduł analizy w czasie rzeczywistym musi być aktualizowany niezależnie od ochrony antywirusowej poprzez konsolę zarządzającą oraz niezależnie, w postaci pliku exe, który można bezpośrednio uruchomić na kliencie	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
23.	Automatyczna rejestracja w dzienniku zdarzeń wszelkich nieautoryzowanych prób zmian rejestru dokonywanych przez użytkownika.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
24.	Automatyczne ponowne uruchomienie skanowania w czasie rzeczywistym, jeśli zostało wyłączone przez użytkownika mającego odpowiednie uprawnienia na z góry określony czas.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
25.	Automatyczne wymuszanie na kliencie programu pobrania zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
26.	Aktualizacje definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
27.	Skanowanie poczty klienckiej (na komputerze klienckim)	<input type="checkbox"/> Tak <input type="checkbox"/> Nie

28.	Opóźnienie skanowania zaplanowanego w wypadku działania komputera (laptopa) na bateriach	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
29.	Ściągnięcie dowolnego pliku na komputer musi spowodować sprawdzenie reputacji takiego pliku – jako reputacja rozumie się odpowiedź, co do ilości użytkowników w Internecie korzystających z danej aplikacji/pliku, czasu, kiedy aplikacja/plik pojawiła się w Internecie po raz pierwszy, oraz czy aplikacja/plik jest „dobra” czy też nie	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
30.	Produkt musi umożliwić utworzenie grup, które będą miały prawo uruchamiać ściągniętą aplikację, jeżeli będzie z niej korzystał w Internecie zdefiniowana ilość użytkowników (przynajmniej: 5, 50, 100, setki użytkowników) oraz dana aplikacja będzie widziana w Internecie od określonej ilości dni	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
31.	W Windows 8 i Windows 10 wsparcie dla funkcji ELAM (Early Launch Anti-Malware) poprzez dostarczenie odpowiedniego sterownika ELAM.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
32.	Dedykowany moduł wywoływany lokalnie lub zdalnie na żądanie z serwera zarządzającego wykonujący agresywne czynności naprawcze w przypadku infekcji na komputerze.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
33.	Dla systemów typu Windows Embedded wsparcie dla Windows Embedded write filters w tym dla File-Based Write Filter (FBWF)	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
34.	System musi posiadać możliwość emulacji w celu analizy polimorficznego złośliwego oprogramowania.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
35.	System musi być wyposażony w dynamiczny klasyfikator próbek wykorzystujący mechanizmy uczenia maszynowego (Machine Learning) w celu wykrywania nowych wersji znanych rodzin złośliwego oprogramowania. Zbiór danych wykorzystywany w algorytmach uczących musi pochodzić z sieci składającej się z co najmniej 150mln sond. Musi istnieć możliwość konfiguracji agresywności (czułości) mechanizmu Machine Learning zarówno w zakresie poziomu, powyżej którego zostanie zgłoszony alarm jak również w zakresie poziomu, powyżej którego system podejmie akcje remediacyjne.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Zapora ogniowa – system Firewall		
1.	Pełne zabezpieczenie stacji klienckich przed: atakami hakerów oraz nieautoryzowanymi próbami dostępu do komputerów i skanowaniem jego portów.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	Moduł firewall ma mieć możliwość monitorowania i kontroli, jakie aplikacje łączą się poprzez interfejsy sieciowe.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Administrator może definiować połączenia, które stacja robocza może inicjować i odbierać.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
4.	Administrator może konfigurować dostęp stacji do protokołów rozszerzonych innych niż ICMP, UDP czy TCP np.: IGMP, GRE, VISA, OSPFIGP, L2TP, Lite-UDP,	<input type="checkbox"/> Tak <input type="checkbox"/> Nie

5.	Program ma pozwalać na zdefiniowanie indywidualnych komputerów lub całych zakresów adresów IP, które są traktowane, jako: całkowicie bezpieczne lub niebezpieczne.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
6.	Program musi wykrywać próby wyszukiwania przez hakerów luk w zabezpieczeniach systemu w celu przejęcia nad nim kontroli.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
7.	Konfiguracja zezwalanego i zabronionego ruchu ma się odbywać w oparciu o takie informacje jak: interfejs sieciowy, protokół, stacja docelowa, aplikacja, godzina komunikacji.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
8.	Konfiguracja stacji ma się odbywać poprzez określenie: Adresu MAC, numeru IP, zakresu numerów IP, wskazanie podsieci, nazwy stacji DNS (FQDN) lub domeny DNS.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
9.	Firewall powinien umożliwiać nagrywanie komunikacji spełniającej wskazane wymagania.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
10.	Firewall ma mieć konfigurowalną funkcjonalność powiadamiania użytkownika o zablokowanych aplikacjach. Ma istnieć możliwość dodania własnego komunikatu.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
11.	W przypadku wykrycia zdefiniowanego ruchu, firewall ma wysłać wiadomość do administratora.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
12.	Uniemożliwianie określenia systemu operacyjnego i rodzaju przeglądarki internetowej przez serwery www.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
13.	Uniemożliwienie określenia systemu operacyjnego poprzez analizę pakietów sieciowych wysyłanych przez stację.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
14.	Uniemożliwienie przejęcia sesji poprzez losowo generowane numery sekwencji TCP.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
15.	Domyślne reguły zezwalające na ruch DHCP, DNS, WINS.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Ochrona przed włamaniami – system IPS		
1.	Producent ma dostarczyć bibliotekę ataków i podatności (sygnatur) stosowanych przez produkt. Administrator ma mieć możliwość uaktualniania tej biblioteki poprzez konsolę zarządzającą oraz niezależnie, w postaci pliku exe, który można bezpośrednio uruchomić na kliencie.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	Biblioteka ataków i podatności musi zawierać przynajmniej 4500 sygnatur.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Biblioteka sygnatur musi zawierać również sygnatury dotyczące działalności programów P2P.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
4.	Produkt ma mieć możliwość tworzenia własnych wzorców włamań (sygnatur), korzystając z semantyki Snort'a. Sygnatury te mogą działać w trybie blokuj lub rejestruj.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
5.	Wykrywanie skanowania portów	<input type="checkbox"/> Tak

		<input type="checkbox"/> Nie
6.	Ochrona przed atakami typu odmowa usług (Denial of Service)	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
7.	Blokowanie komunikacji ze stacjami z podmienionymi MAC adresami (spoofed MAC)	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
8.	Wykrywanie trojanów i generowanego przez nie ruchu	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
9.	Wykrywanie prób nawiązania komunikacji za pośrednictwem zaufanych aplikacji, przez inne oprogramowanie.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
10.	Blokowanie komunikacji ze stacjami uznanymi za wrogie na zdefiniowany przez administratora czas. Ma istnieć możliwość definiowania wyjątków	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
11.	System ochrony przed włamaniami musi automatycznie integrować się z przeglądarką internetową (przynajmniej z Internet Explorer oraz Firefox) – uniemożliwiając wykonanie w nich (nawet, jeżeli są podatne) szkodliwego dla nich kodu	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
12.	System musi posiadać mechanizm blokowania wykorzystywania nieznanych podatności w określonym oprogramowaniu (Exploit Prevention) co najmniej dla aplikacji pakietu Office, Firefox, Internet Explorer oraz aplikacji napisanych w języku Java a także VLC. System musi implementować co najmniej 10 technik ochrony w tym następujące metody prewencji: <ul style="list-style-type: none"> • Java Exploit Protection • Structured Exception Handling Overwrite Protection (SEHOP) • Heap Spray Memory Attack • Forced DEP • Forced ASLR • Anti-ROP 	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Ochrona systemu operacyjnego		
1.	Produkt ma umożliwiać uruchamianie i blokowanie wskazanych aplikacji	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	Produkt ma umożliwiać ładowanie modułów lub bibliotek DLL	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Produkt ma umożliwiać kontrolę odczytywania i zapisywania na systemie plików przez wskazane aplikacje	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
4.	Aplikacje powinny być rozróżniane poprzez nazwę i sygnaturę cyfrową	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
5.	Produkt ma umożliwiać blokowanie wskazanego typu urządzeń przed dostępem użytkownika – urządzenia muszą być identyfikowane po ich numerze seryjnym	<input type="checkbox"/> Tak <input type="checkbox"/> Nie

6.	Produkt ma kontrolować dostęp do rejestru systemowego	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
7.	Produkt ma umożliwiać logowanie plików wgrywanych na urządzenia zewnętrzne	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
8.	Produkt musi automatycznie umożliwić zablokowanie pliku autorun.inf na urządzeniach zewnętrznych i na udziałach sieciowych	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
9.	Polityki ochrony mają mieć możliwość pracy w dwóch trybach, testowym i produkcyjnym. W trybie testowym aplikacje i urządzenia nie są blokowane, ale jest tworzony wpis w logu	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
10.	Możliwość wykluczenia dowolnej aplikacji z trybu ochrony systemu operacyjnego	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
11.	Możliwość utworzenie listy zaufanych aplikacji (tzw. białej listy) i konfiguracji produktu w taki sposób, by żadna inna aplikacja/biblioteka spoza listy nie mogła uruchomić się na komputerze	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
12.	Kolekcja aktualnie znajdujących się aplikacji na systemie końcowym musi być możliwa do wywołania bezpośrednio z konsoli zarządzającej – bez konieczności wykonania jakichkolwiek czynności na systemie końcowym	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
13.	Możliwość utworzenia listy blokowanych aplikacji (tzw. czarnej listy) i konfiguracji produktu w taki sposób, by tylko aplikacja znajdujące się na liście nie mogły uruchomić się na komputerze	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
14.	Możliwość automatycznego importu list zarówno białej, jak i czarnej, co zdefiniowany interwał czasu	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Mechanizm pułapek:		
1.	System musi posiadać wbudowany mechanizm pułapek pozwalający na detekcję zaawansowanych ataków poprzez obserwowanie sztucznie wytworzonych zasobów - przynęt.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	System powinien umożliwiać zdefiniowanie następujących przynęt: <ul style="list-style-type: none"> • Użytkownika – przynętą są sztucznie spreparowane informacje uwierzytelniające dla użytkownika. Każda próba użycia tych informacji uwierzytelniających powinna generować alarm. • Proces – przynęta imituje działanie procesu innego systemu ochrony. Każda próba zatrzymania sztucznego procesu powinna generować alarm. • Udział sieciowy – powinna wykrywać próby połączenia z nieistniejącym, ale specjalnie spreparowanym udziałem sieciowym. Każda próba dostępu do udziału powinna generować alarm. • IP – przynęta polegająca na sztucznym wstrzyknięciu do systemu operacyjnego informacji o nieistniejącym adresie IP. System powinien wygenerować alarm w przypadku próby połączenia z adresem-przynętą. • DNS – przynęta polegająca na wstrzyknięciu w system operacyjny sztucznej domeny. Każda próba dostępu do tej domeny powinna generować alarm. 	<input type="checkbox"/> Tak <input type="checkbox"/> Nie

3.	System powinien samodzielnie ustawiać i usuwać przynęty w zależności od konfiguracji polityki. Konfiguracja powinna być dostępna z interfejsu administracyjnego rozwiązania.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
4.	Mechanizm pułapek powinien mieć wspólny panel raportowania z pozostałymi elementami systemu.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Integralności komputera:		
1.	Oprogramowanie musi umożliwiać wykonywanie szerokiego zakresu testów integralności komputera pod kątem zgodności z polityką bezpieczeństwa urządzeń końcowych, w tym: programów antywirusowych, poprawki firmy Microsoft, dodatki Service Pack firmy Microsoft, osobistych zapór ogniowych	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	Testy integralności ma być przeprowadzany cyklicznie, co zdefiniowany okres czasu.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Powyższe szablony muszą być automatycznie aktualizowane ze strony producenta	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
4.	Oprogramowanie musi umożliwiać wykonanie niestandardowego (dowolnie zdefiniowanego) testu integralności komputera, posiadać zaawansowaną składnię If...Then...Else.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
5.	<p>W przypadku niestandardowego testu integralności musi istnieć dostępność następujących testów:</p> <ul style="list-style-type: none"> • Wpisy rejestru systemu operacyjnego - istnienie, określona wartość, inne • Pliki - istnienie, data, rozmiar, suma kontrolna • Wiek, data, rozmiar pliku sygnatury oprogramowania antywirusowego • Zainstalowane poprawki • Uruchomiony proces, wersja systemu operacyjnego • Własny skrypt VisualBasic, wsh, itp. • Własna aplikacja 	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
6.	<p>W przypadku niezgodności stacji z testem integralności, musi być możliwość ustawienia akcji naprawczej na poziomie pojedynczego testu. Jako możliwe operacje do wykonania, musi istnieć możliwość:</p> <ul style="list-style-type: none"> • Uruchamianie dowolnego/własnego skryptu lub programu • Logowanie zdarzenia • Ukazanie okienka z wiadomością • Pobieranie oraz uruchamianie instalacji 	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
7.	Ma istnieć możliwość wskazania czasu oczekiwania na wykonanie akcji naprawczych.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
8.	Możliwość wymuszenia instalacji dowolnej aplikacji.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie

9.	W wypadku niezgodności własnego systemu, oprogramowanie musi umożliwić zaaplikowanie dowolnego innego zestawu konfiguracji, w szczególności polityki firewallowej (zdefiniowanej bardzo restrykcyjnie), polityki antywirusowej, polityki pobierania aktualizacji, polityki kontroli uruchamianych aplikacji i polityki kontroli urządzeń.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
10.	Musi być możliwe, nieuwzględnianie wyniku poszczególnego testu na wynik końcowy integralności komputera.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
11.	Musi istnieć możliwość stwierdzenia, że na komputerze znaleziono zagrożenie i nie można było takiego zagrożenia usunąć – na ten czas komputer powinien znaleźć się w kwarantannie.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
12.	Musi istnieć test integralności komputera, który sprawdzi czy komputer nie jest podłączony do Internetu poprzez dwie różne drogi, np. poprzez kabel sieciowy (Ethernet) i poprzez dostęp mobilny (WIFI, modem GSM, etc.)	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Ochrona środowisk wirtualnych		
1.	Produkt musi umożliwiać identyfikację środowiska wirtualnego, w którym działa, informacja na ten temat musi być widoczna w konsoli. Minimalnie identyfikowane środowiska to: Citrix, Microsoft, VMWare	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	Produkt musi umożliwiać w wypadku skanowania w czasie rzeczywistym oraz przy skanowaniu zaplanowanym, wykluczenie w środowisku wirtualnym wszystkich plików z tzw. złotego obrazu (Gold Image) - nie będą one nigdy poddawane skanowaniu	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Produkt musi umożliwiać współdzielenie wyników skanowania zaplanowanego i na żądanie pomiędzy instancjami wirtualnymi - znalezienie już raz przeskanowanego tego samego pliku powoduje nieskanowanie go na systemie pytającym. Technologia ta powinna być dostępna, jako oprogramowanie instalowane w systemie operacyjnym Windows	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
4.	Produkt musi umożliwiać prawidłowe rozliczenia licencji oferowanego systemu dla systemów wirtualnych typu desktop tzw. VDI, w szczególności tzw. „non-persistent”	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
5.	Produkt musi umożliwiać przeskanowanie plików vmdk w poszukiwaniu zagrożeń	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
6.	System musi posiadać specjalne, dedykowane sygnatury do ochrony środowisk wirtualnych. Sygnatury takie powinny się cechować przede wszystkim zmniejszonym zapotrzebowaniem na przestrzeń dyskową po zainstalowaniu oraz zmniejszonym zapotrzebowaniem na przepustowość sieci wymagającą do aktualizacji.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Architektura		
1.	Rozwiązanie ma mieć architekturę trój-warstwową. Klienci mają być zarządzani przez serwery, a konfiguracja rozwiązania ma być zapewniona poprzez graficzną konsolę administratora.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	Rozwiązanie ma zapewniać wysoką skalowalność i odporność na awarie.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Komunikacja pomiędzy agentami i serwerem ma być szyfrowana.	<input type="checkbox"/> Tak

		<input type="checkbox"/> Nie
4.	Numery portów używane do komunikacji mają mieć możliwość konfiguracji przez użytkownika końcowego.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
5.	Agent ma się przełączać do innego serwera zarządzającego w przypadku niedostępności przypisanego serwera.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
6.	Serwery zarządzające mają móc replikować pomiędzy sobą informacje o agentach, ich konfiguracji oraz logi. Musi istnieć możliwość zdefiniowania kierunku replikacji logów (jednostronna lub dwustronna).	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
7.	Musi istnieć możliwość zdefiniowania dowolnego klienta, jako lokalnego dostawcy aktualizacji – możliwość konfiguracji ilości przetrzymywanych aktualizacji, zajętości na dysku oraz konfiguracji prędkości ich pobierania z serwera zarządzającego.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
8.	Definiowanie lokalnego repozytorium musi zawierać warunki, jakie muszą być zachowane by dany komputer mógł stać się lokalnym repozytorium – warunkami muszą być przynajmniej: wersja systemu operacyjnego, adres komputera, nazwa komputera (z możliwością podania ją ze znakami specjalnymi, np.: komputer*), określonego wpisu w rejestrze.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
9.	Możliwość manualnego wskazania wybranej grupie komputerów konkretnego lokalnego dostawcy aktualizacji.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
10.	Możliwość uruchomienia dedykowanego narzędzia służącego do monitorowania klientów, którzy zostali lokalnymi dostawcami aktualizacji. Monitorowane jest ich zdrowie, ilość ściągniętych od nich danych, czy były to ściągnięte pełne definicje czy też definicje przyrostowe.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
11.	Możliwość ograniczenia pasma sieciowego od serwera zarządzającego do jego klientów w zależności od ściąganych definicji, aktualizacji klienckiej, podsieci, z której się łączą.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Moduł raportujący:		
1.	Produkt ma zapewniać graficzne raportowanie.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	Wbudowane raporty mają pokazywać: <ul style="list-style-type: none"> • stan dystrybucji sygnatur antywirusowych, sygnatur heurystycznych oraz IDS/IPS, • wersje zainstalowanych klientów, • inwentaryzacje stacji roboczych (w tym wielkość dysku, zajętość dysku, wielkość pamięci RAM, wykorzystywany system operacyjny oraz procesor), • wykrytych wirusów, zdarzeń sieciowych, integralności komputerów, • zainstalowane technologie i ich aktualny stan. 	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Moduł raportowania ma pokazywać stan wykonywanych poleceń na komputerach.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie

4.	Możliwość zaplanowanego tworzenia raportów i przesyłania ich do danych kont pocztowych.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
5.	Produkt musi umożliwiać automatyczne zbudowanie zapytań, które będą wykonywane o zdany czas i ich wynik będzie przechowywany w postaci kostek OLAP. Powstałe kostki muszą umożliwiać wykonywanie na nich typowych operacji takich jak zwiżanie/agregacja danych, rozwijanie (bardziej szczegółowe dane), selekcja (wybór interesujących danych). Wszystkie te operacje muszą być wykonywane graficznie.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
6.	Produkt musi umożliwiać automatyczne budowanie trendów.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
7.	Produkt musi umożliwiać automatyczne budowanie kluczowych wskaźników wydajności (KPI).	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Moduł centralnego zarządzania:		
1.	Centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem z pojedynczej konsoli.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	Centralna aktualizacja ochrony antywirusowej, zapory ogniowej i systemu wykrywania włamań przez administratora sieci.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Produkt ma wykrywać i raportować nieautoryzowane zmiany w konfiguracji produktu na stacji roboczej. Ma istnieć możliwość blokowania takich zmian.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
4.	Produkt ma zapewniać zarządzanie poprzez konsolę. Dostęp do konsoli ma być możliwy po wcześniejszej weryfikacji użytkownika. Produkt ma mieć możliwość definiowania wielu kont administracyjnych i niezależną konfigurację uprawnień.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
5.	Możliwość definiowania wielu niezależnych organizacji na jednym serwerze zarządzającym – informacje dostarczone do serwera zarządzającego nie będą dostępne pomiędzy organizacjami	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
6.	Integracja z Microsoft Active Directory w celu importu użytkowników, listy maszyn, struktury jednostek organizacyjnych.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
7.	Konta administracyjne mają być tworzone na poziomie serwerów zarządzających i na poziomie organizacji definiowanych na serwerze.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
8.	Uprawnienia administratorów mają być ustawiane niezależnie dla każdego kontenera wewnątrz organizacji.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
9.	Możliwość utworzenia administratorów z uprawnieniami tylko do odczytu.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
10.	Konfiguracja agentów ma mieć strukturę drzewa, z mechanizmami dziedziczenia.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
11.	Uwierzytelnianie administratorów ma się odbywać w oparciu o wewnętrzną bazę danych lub z użyciem Microsoft Active Directory. Produkt ma mieć	<input type="checkbox"/> Tak <input type="checkbox"/> Nie

	możliwość wykorzystania wieloelementowego uwierzytelniania (np. z wykorzystaniem tokenów, certyfikatów itp.)	
12.	Dostęp do interfejsu produktu i listy funkcji dostępnych dla użytkownika ma być konfigurowany z poziomu centralnej konsoli zarządzającej.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
13.	Konfiguracja aktywna na stacji ma rozróżniać lokalizację agenta i według tego kryterium określać stosowany zestaw reguł/polityk dla agenta.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
14.	Lokalizacja ma być określana według istnienia lub nieistnienia: typu interfejsu sieciowego, numeru MAC domyślnej bramki, adresu IP, zakresu podsieci, wartości kluczy w rejestrze, komunikacji z serwerem zarządzającym, nazwy domeny, adresów serwerów WINS, DNS, DHCP, wyniku zapytania do serwera DNS.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
15.	Opis lokalizacji powinien zawierać możliwość tworzenia połączeń logicznych „I” oraz „LUB” na powyżej wymienionych elementach.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
16.	Paczki instalacyjne produktu mają pozwalać na dodanie własnej konfiguracji.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
17.	W paczce instalacyjnej musi być zawarta funkcjonalność deinstalacji innych produktów bezpieczeństwa, która uruchomi się automatycznie przed instalacją produktu.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
18.	Pełna funkcjonalność ma być zawarta w jednym pliku instalacyjnym.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
19.	Nowe wersje oprogramowania mają być automatycznie dystrybuowane na stacje robocze w postaci różnicy między aktualnie zainstalowaną wersją na kliencie a nową wersją oprogramowania.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
20.	Produkt ma automatycznie wykrywać wszystkie urządzenia przyłączone do sieci komputerowej.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
21.	Możliwość zdefiniowania alertów administracyjnych zawierających zdarzenia: <ul style="list-style-type: none"> • błędnej autoryzacji do systemu zarządzania, • dostępności nowego oprogramowania, • pojawienia się nowego komputera, • zdarzeń powiązanych z infekcjami wirusów, • stanu serwerów zarządzających. 	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
22.	Możliwość konfiguracji przepustowości pasma pomiędzy klientami a serwerem zarządzającym osobna dla pobieranych definicji przyrostowych, pełnych i pakietów aktualizacji.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
23.	Oficjalna dokumentacja schematu bazy danych, z której korzysta system zarządzający.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
24.	Pełna polska wersja językowa oprogramowania dla systemu zarządzania i stacji klienckich wraz z dokumentacją.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie

Platforma:		
1.	<p>Oprogramowanie musi działać na systemach:</p> <ul style="list-style-type: none"> • Windows 11 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025 	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	<p>Komponenty rozwiązania takie jak: firewall, zapobieganie włamaniom, kontrola urządzeń i aplikacji oraz kontrola integralności komputera muszą działać na wszystkich powyższych platformach 32 i 64-bitowych.</p>	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	<p>Serwer zarządzający musi działać na systemach:</p> <p>Windows Server w wersji min. 2019 lub nowszym, objętym oficjalnym wsparciem producenta, w wersji 64-bitowej.</p>	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Ochrona antywirusowa dla systemu Linux		
1.	<p>Ochrona antywirusowa z pominięciem funkcji reputacji ma działać na platformie:</p> <ul style="list-style-type: none"> • AlmaLinux / Rocky Linux: wersje 8.x oraz 9.x • Red Hat Enterprise Linux Server (RHEL): RHEL 8.x, RHEL 9.x • Oracle Linux (OEL): Oracle Linux 8.x, 9.x • Debian: Debian 11 (bullseye), Debian 12 (bookworm) • Ubuntu LTS: Ubuntu 20.04 LTS, 22.04 LTS, 24.04 LTS • SUSE Linux Enterprise Server (SLES): SLES 15 (SP3–SP5) • Fedora (środowiska nieprodukcyjne / developerskie): Fedora 40, Fedora 41 	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	<p>Klient dla system Linux ma być zarządzany przez ten sam serwer oraz z tej samej konsoli zarządzającej, co klienci Windows</p>	<input type="checkbox"/> Tak <input type="checkbox"/> Nie

CZĘŚĆ II – OCHRONA URZĄDZEŃ MOBILNYCH

Przedmiotem zamówienia w Części II jest odnowienie wsparcia producenta do posiadanych licencji systemów bezpieczeństwa dla urządzeń mobilnych wraz z centralną konsolą zarządzającą albo dostawa oprogramowania równoważnego.

W chwili obecnej Zamawiający posiada wymienione w tabeli nr 2 licencje na produkty firmy ESET. W ramach niniejszego zamówienia, Zamawiający wymaga przedłużenia wsparcia producenta do posiadanych licencji w okresie od dnia 01 sierpnia 2026 r. do dnia 31 lipca 2027 r. Dostarczone przez Wykonawcę wsparcie producenta ma umożliwić bezpłatne wykonanie aktualizacji posiadanych licencji, do najnowszej wersji oprogramowania.

Tabela nr 2 – Tabela dot. specyfikacji ESET PROTECT Essential

Lp.	Opis produktu	Identyfikator Licencji	Ilość licencji
1	ESET PROTECT Essential (aktualnie najnowsza wersja produktu)	3AX-V9P-4N7	800

W wypadku zaoferowania oprogramowania równoważnego oferent odpowiedzialny jest za:

- migracje całego środowiska do zaoferowanego oprogramowania,
- migracji polityk (antywirusowych, wykluczeń, polityk zapory ogniowej, polityk kontroli aplikacji i urządzeń),
- przeprowadzenie szkoleń dla administratorów systemu, w zakresie używania nowego systemu, jaki i w zakresie przeprowadzonej implementacji

Implementacja musi zostać udokumentowana dokumentem po wdrożeniowym zawierającym:

- implementację,
- procedury odzyskiwania całego środowiska.

Tabela nr 2.1 - Tabela dot. specyfikacji rozwiązania równoważnego

LP	Minimalne wymagania dla oprogramowania równoważnego dla pozycji 1 z tabeli nr. 2: producent i nazwa produktu: wypełnia Wykonawca ilość: wypełnia Wykonawca	Deklaracja zgodności z opisem wymagań minimalnych Wstawić znak „X” we właściwą kratkę.
Ochrona urządzeń mobilnych opartych o system Android		
1.	Rozwiązanie musi wspierać system co najmniej Android 6.0	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	Rozwiązanie musi wspierać rozdzielczość wyświetlacza urządzenia 480x800px lub wyższą.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Rozwiązanie musi wspierać procesory: ARM z obsługą ARMv7 lub x86 Intel Atom.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie

4.	Rozwiązanie musi posiadać ochronę plików w czasie rzeczywistym.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
5.	Rozwiązanie musi posiadać ochronę przed atakami typu „phishing”.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
6.	Rozwiązanie musi skanować wszystkie typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
7.	Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
8.	Rozwiązanie musi posiadać ochronę proaktywną wykrywającą nieznane zagrożenia.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
9.	W przypadku wykrycia zagrożenia użytkownik musi otrzymać odpowiednie powiadomienie.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
10.	Rozwiązanie musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia przez administratora z poziomu konsoli zarządzającej.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
11.	Rozwiązanie musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Skanowanie na żądanie		
1.	Rozwiązanie musi mieć możliwość skanowania zainstalowanych aplikacji.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	Informacje o skanowaniu mają być przechowywane w plikach dziennika.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
4.	Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Ochrona przed kradzieżą		
1.	Administrator ma mieć możliwość skonfigurowania zaufanej karty SIM.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	<p>W przypadku kradzieży urządzenia, Administrator ma mieć możliwość zdalnie wysłania na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:</p> <ul style="list-style-type: none"> a) usunięcie zawartości urządzenia, b) przywrócenie urządzenie do ustawień fabrycznych, c) zablokowania urządzenia, 	<input type="checkbox"/> Tak <input type="checkbox"/> Nie

	d) uruchomienie sygnału dźwiękowego, e) lokalizację GPS	
Polityka ustawień		
1.	Administrator musi mieć wgląd w podstawowe ustawienia urządzenia z konsoli centralnego zarządzania, w tym co najmniej: a) połączenie Wi-Fi, b) GPS, c) usługi lokalizacyjne, d) pamięć, e) roaming danych, f) nieznane źródła, g) tryb debugowania, h) komunikacja NFC, i) szyfrowanie pamięci masowej, j) urządzenie zrotowane.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Kontrola aplikacji		
1.	Rozwiązanie musi umożliwiać administratorowi z konsoli centralnego zarządzania podejrzenie listy zainstalowanych aplikacji	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	Administrator z konsoli centralnego zarządzania musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Blokowanie aplikacji musi być możliwe w oparciu o: a) nazwę aplikacji, b) nazwę pakietu, c) kategorię sklepu Google Play, d) uprawnienia aplikacji, e) pochodzenie aplikacji z nieznanego źródła.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Zabezpieczenia urządzenia		
1.	W ramach zabezpieczeń administrator z konsoli centralnego zarządzania musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej: a) minimalny poziom zabezpieczeń i złożoność blokady ekranu, b) maksymalną dopuszczaną liczbę błędnych prób odblokowania, c) odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie, d) czas, po którym automatycznie nastąpi blokada ekranu e) ograniczenie dostępu do kamery wbudowanej w urządzenie.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Aktualizacje modułów		

1.	Rozwiązanie musi umożliwiać wymuszenie pobrania aktualizacji na żądanie z konsoli centralnego zarządzania.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	Rozwiązanie musi mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje modułów co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Rozwiązanie musi posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Konfiguracja i zdalne zarządzanie		
1.	Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
4.	Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
5.	Wdrożenie urządzenia mobilnego z poziomu konsoli zarządzającej musi się odbyć co najmniej na jeden z trzech możliwych sposobów: a) za pomocą kodu QR, b) za pomocą unikatowego łącza, c) za pomocą wiadomości e-mail	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
Centralna konsola zarządzająca		
1.	Musi być rozwiązaniem możliwym do uruchomienia na infrastrukturze u Zamawiającego.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
2.	Musi umożliwiać działanie w oparciu o wirtualizator VMware esxi w wersji co najmniej 7.0.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
3.	Musi umożliwiać podział klientów na grupy z co najmniej trzema poziomami zagnieżdżenia.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
4.	Dostęp do konsoli musi być realizowany za pomocą technologii www.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie
5.	Konsola musi posiadać możliwość integracji z serwerem LDAP lub RADIUS w celu uwierzytelnienia użytkowników.	<input type="checkbox"/> Tak <input type="checkbox"/> Nie