Załącznik nr 1 do SWZ

Szczegółowy opis przedmiotu zamówienia

I. Przedmiot zamówienia

Przedmiotem zamówienia jest:

1) odnowienie usługi wsparcia technicznego producenta dla McAfee Complete EndPoint Protection – Business – w ilości 900 szt. ważnej od dnia 26 maja 2022 r. przez okres 36 miesięcy;
2) dostawa licencji McAfee Complete EndPoint Protection – Business – w ilości 150 szt. ważnych od dnia 26 maja 2022 r. przez czas nieoznaczony wraz z usługą wsparcia technicznego producenta na okres 36 miesięcy;
3) odnowienie subskrypcji McAfee MVISION TIE – w ilości 800 szt. ważnych od dnia 26 maja 2022 r. przez okres 36 miesięcy;
4) dostawa subskrypcji McAfee MVISION TIE – w ilości 100 szt. ważnych od dnia 26 maja 2022 r. przez okres 36 miesięcy;
5) odnowienie subskrypcji McAfee Virtual Advanced Threat Defence Appliance – w ilości 1 szt. ważnej od dnia 26 maja 2022 r. przez okres 36 miesięcy,

lub dostawa rozwiązania równoważnego.

II. Opis rozwiązania równoważnego

1) Zamawiający posłużył się nazwą własną producenta dla ułatwienia opisu przedmiotu zamówienia, w oparciu o przesłanki art. 99 ust. 5 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r., poz. 1129 ze zm.).
2) Zaoferowane rozwiązanie równoważne musi spełniać następujące kryteria minimalne:

1. Wymagania ogólne:

Lp.	Konfiguracja minimalna
1.	Rozwiązanie musi wspierać, co najmniej następującą platformę wirtualizacyjną (jeżeli zostanie dostarczony w postaci maszyn wirtualnych): VMware.
2.	Rozwiązanie musi wspierać następujące klienckie systemy operacyjne: a) Windows 7 (wersja x32 i x64) b) Windows 8 i 8.1 (wersja x32 i x64) c) Windows 10 (wersja x32 i x64) Rozwiązanie musi wspierać następujące serwerowe systemy operacyjne: a) Windows Server 2012/2012 R2 b) Windows Server 2016/2016 R2 c) Windows Server 2019
3.	Zaproponowane rozwiązanie musi zapewniać ochronę w zakresie: a) Kompleksowej ochrony stacji końcowych i serwerów przed złośliwym kodem/oprogramowaniem, uruchamianiem aplikacji, ochroną przed podatnościami usług, wyciekiem danych, podłączaniem nieznanych urządzeń. b) Zapewnieniem poufności danych poprzez możliwość szyfrowania systemów plików (filesystems), całych dysków, jak i pojedynczych plików znajdujących się na dyskach twardych (m.in.: HDD, SSD - lista niewyczerpująca) oraz nośnikach zewnętrznych

	(m.in. pendrive, inne dyski podłączane poprzez port USB, karty pamięci - lista niewyczerpująca). c) Ochrony na poziomie sieciowym, analiza ruchu webowego i wiadomości pocztowych w kontekście ochrony przed wyciekiem danych, złośliwego kodu, spamu i reputacji.
4.	Rozwiązanie musi pozwalać na swobodne przekazanie zdarzeń do zewnętrznych repozytoriów logów przy pomocy formatu syslog CEF/LEEF.
5.	Rozwiązanie musi umożliwiać uruchomienie serwera do obsługi stacji roboczych znajdujących się poza siecią lokalną Zamawiającego. Serwer taki musi być przystosowany do pracy w DMZ.
6.	Zaproponowane rozwiązanie w przypadku, gdy składa się z komponentów różnych producentów, musi stanowić jedną całość, gdzie poszczególne komponenty nie utrudniają sobie wzajemnie pracy, nie wypaczają działania mechanizmów innych modułów a użycie komponentów różnych producentów nie obniża poziomu bezpieczeństwa infrastruktury Zamawiającego.
7.	Wszystkie moduły rozwiązania muszą komunikować się między sobą w bezpieczny sposób (transmisja pomiędzy maszynami musi być szyfrowana).

2. Moduł szyfrowania dysków:

Lp.	Konfiguracja minimalna
1.	System szyfrowania musi zapewniać centralne zarządzanie poprzez Centralną Konsolę Zarządzania (dalej CKZ) co najmniej w zakresie szyfrowania danych, w oparciu o centralną bazę danych, gdzie przetrzymywane są informacje o użytkownikach, kluczach i politykach szyfrowania niezbędne do uzyskania dostępu do danych zaszyfrowanych na stacji w sytuacji awaryjnej.
2.	Rozwiązanie musi zapewnić szyfrowanie danych na poziomie dysku w sposób transparentny dla systemu operacyjnego i użytkowników, z możliwością uruchomienia funkcjonalności uwierzytelniania użytkownika bezpośrednio po uruchomieniu komputera (przed wystartowaniem właściwego systemu operacyjnego - tzw. pre-boot authentication, zwany dalej PBA).
3.	Oprogramowanie szyfrujące na stacjach końcowych musi komunikować się z CKZ w bezpieczny sposób (transmisja szyfrowana).
4.	Rozwiązanie musi obsługiwać, co najmniej algorytm AES 256, jako algorytm szyfrowania danych.
5.	Uwierzytelnianie użytkownika w PBA ma być możliwe z wykorzystaniem hasła i nazwy użytkownika.
6.	System musi pobierać użytkowników z domeny opartej o Active Directory (AD) oraz dać możliwość ręcznej definicji użytkowników niezależnie od AD. System musi umożliwiać wskazanie, który użytkownik i grupa mają prawo używać komputer i uzyskać dostęp do zaszyfrowanych danych: a) użytkownicy i grupy użytkowników przypisywani do komputerów muszą być synchronizowani z domeny Microsoft Active Directory, b) usunięcie użytkownika w serwerze usług katalogowych AD musi skutkować automatycznym usunięciem lub zablokowaniem użytkownika w serwerze zarządzającym systemem szyfrowania.
7.	Zmiany hasła użytkownika na jednej maszynie muszą być automatycznie powielane i synchronizowane na pozostałych komputerach, do których jest przypisany ten użytkownik.
8.	Zmiana hasła z poziomu systemu Windows musi być automatycznie replikowana do systemu szyfrującego tak, by nie było potrzeby dwukrotnej zmiany hasła.

9.	Rozwiązanie musi umożliwiać pracę w trybie single sign-on (SSO) – po zalogowaniu się w trybie PBA użytkownik nie musi już logować się po raz kolejny do systemu Windows, jego dane są automatycznie przekazywane przez moduł PBA do procesu logowania Windows.
10.	System musi zapewnić centralne przechowywanie kluczy użytych do szyfrowania danych i umożliwić odzyskanie zaszyfrowanych danych z ich wykorzystaniem w sytuacji awaryjnej.
11.	Każdy komputer musi posiadać swój unikalny klucz wykorzystywany do szyfrowania danych na dysku oraz powinien być obecny w bazie CKZ.
12.	Oprogramowanie szyfrujące musi kontynuować pracę po niespodziewanym zaniku zasilania, bez wpływu na możliwość zaszyfrowania i odszyfrowania danych.
13.	System musi zapewniać możliwość centralnej konfiguracji parametrów szyfrowania, w tym centralne ustalanie polityk dla użytkowników i komputerów.
14.	Stacje i użytkownicy muszą synchronizować zmiany w politykach szyfrowania oraz parametrach systemu bez konieczności interwencji administratora.
15.	System przed rozpoczęciem szyfrowania musi sprawdzić, czy na komputerze nie znajduje się oprogramowanie niekompatybilne.
16.	System musi umożliwiać generowanie raportów dotyczących, co najmniej: stanu zaszyfrowania systemu (stacja nie zaszyfrowana, stacja zaszyfrowana, stacja w trakcie szyfrowania), wersji działającego oprogramowania szyfrowania, przypisanych do stacji użytkowników.
17.	System na stacjach końcowych musi umożliwiać zmianę hasła użytkownika w przypadku jego zapomnienia. Proces zmiany hasła musi spełniać, co najmniej jeden z poniższych warunków: a) musi istnieć tryb zmiany hasła nie wymagający podłączenia stacji do sieci firmowej, b) musi istnieć możliwość samodzielnego zresetowania hasła przez użytkownika w trybie PBA w oparciu o podanie odpowiedzi na wcześniej zdefiniowane pytania, podanie tokenu lub z wykorzystaniem podobnych technik.
18.	System musi oferować możliwość wykorzystania wbudowanego w system operacyjny mechanizmu szyfrowania oprócz oferowania własnego mechanizmu szyfrującego. System musi obsługiwać, co najmniej poniższe mechanizmy szyfrowania: a) Bitlocker w przypadku systemów Microsoft Windows,
19.	System musi zapewniać automatyczne szyfrowanie tzw. pliku wymiany Windows (pagefile).
20.	Moduł szyfrowania dysków pozwala na określenie, czy szyfrowaniu mają podlegać wszystkie partycje dysku, czy tylko partycja bootowalna (z której startuje właściwy system operacyjny) lub tylko partycje danych (non-bootable). Musi też istnieć możliwość określenia dowolnej konfiguracji partycji do zaszyfrowania.

3. Moduł szyfrowania plików:

Lp.	Konfiguracja minimalna
1.	Rozwiązanie musi zapewnić: a) szyfrowanie plików i katalogów w ramach systemu operacyjnego i udziałów sieciowych udostępnianych przez serwery sieciowe. b) szyfrowanie danych kopiowanych na dyski twarde oraz nośniki zewnętrzne USB oraz CD/DVD.
2.	System szyfrowania plików i katalogów musi zapewniać centralne zarządzanie, w oparciu o CKZ, co najmniej w obszarze szyfrowania plików.
3.	Oprogramowanie szyfrujące na stacjach końcowych musi komunikować się z CKZ w

	bezpieczny sposób (transmisja szyfrowana).
4.	Rozwiązanie musi obsługiwać, co najmniej algorytm AES 256, jako algorytm szyfrowania danych.
5.	Rozwiązanie musi zapewniać mechanizm odzyskania danych, gdy użytkownik zapomni hasła lub utraci klucz.
6.	Musi istnieć możliwość użycia kluczy wykorzystywanych do szyfrowania plików i katalogów oraz nośników zewnętrznych także w trybie off-line (kiedy stacja nie jest podłączona do sieci Zamawiającego i jeśli nie ma połączenia z centralnym serwerem zarządzającym)
7.	Decyzja o zaszyfrowaniu pliku/katalogu może zostać podjęta w oparciu o: a) centralnie zdefiniowaną politykę wskazująca foldery/pliki obligatoryjnie szyfrowane, b) lokalnie przez użytkownika.
8.	W przypadku centralnie definiowanej polityki musi być możliwe, co najmniej: a) wskazanie plików/folderów, które powinny być obligatoryjnie szyfrowane, b) wskazanie udziałów sieciowych, których pliki powinny być zaszyfrowane. Komunikacja między stacją użytkownika a udziałem sieciowym z zaszyfrowanymi plikami nie może powodować, że pliki lub ich części są przesyłane niezaszyfrowane.
9.	Uwierzytelnianie użytkownika na potrzeby systemu szyfrowania plików musi wykorzystywać uwierzytelnianie Microsoft Windows i umożliwiać przezroczystą pracę dla użytkowników bez potrzeby dodatkowego uwierzytelniania się.
10.	W przypadku, gdy Zamawiający zrezygnuje z mechanizmów uwierzytelniania wbudowanych w Microsoft Windows – powinna istnieć możliwość wykorzystania wbudowanego systemu uwierzytelniania w moduł szyfrowania plików.
11.	Rozwiązanie musi obsługiwać dowolne zewnętrzne nośniki wymienne USB i umożliwiać szyfrowanie na nich plików i katalogów. Powinny istnieć następujące możliwości szyfrowania nośników wymiennych: a) szyfrowanie proste, poprzez wymuszenia szyfrowania kopiowanych plików wprost na nośnik zewnętrzny (każdy wkopiowany plik będzie poddany szyfrowaniu), b) szyfrowanie konkretnego katalogu określonego ścieżką.

4. Oprogramowanie do ochrony stacji końcowych przed zagrożeniami (dalej OOPZ):

Lp.	Konfiguracja minimalna
1.	Pakiet oprogramowania do ochrony stacji komputerowych przed zagrożeniami winno składać się z: a) modułu antywirusowego (dalej AV), b) modułu hostowego firewall'a (dalej FW), c) modułu Host IPS (dalej HIPS), d) modułu ochrony przeglądarek webowych przed złośliwymi stronami web (dalej WP), e) modułu kontroli portów (dalej KP), f) modułu kontroli aplikacji (dalej KA), g) modułu ochrony poczty elektronicznej (dalej OPE), h) modułu sandbox. Rozwiązanie winno posiadać Centralną Konsolę Zarządzającą obsługującą konfigurację, przegląd zdarzeń, itp. co najmniej obejmującą swym zakresem obszar pojedynczych modułów wchodzących w skład OOPZ.
2.	Instalacja OOPZ (co najmniej agenta zarządzającego na stacji końcowej) musi być możliwa poprzez instalację ręczną oraz instalację automatyczną z użyciem konsoli zarządzającej lub zewnętrznego oprogramowania wymagającego plików MSI.

3.	Oprogramowanie OOPZ musi umożliwić pracę w środowiskach całkowicie izolowanych, gdzie nie ma dostępu do Internetu. Musi istnieć możliwość ręcznej aktualizacji wszystkich komponentów wymagający cyklicznej aktualizacji z użyciem CKZ.
4.	W ramach modułów OOPZ muszą być obecne mechanizmy samoobrony przed próbami zatrzymania lub wyłączenia ochrony poprzez te moduły. Muszą być mechanizmy zapobiegające modyfikacjom zarówno struktury plików, procesów, jak i rejestrów niezbędnych do pracy OOPZ. Wszystkie próby zatrzymania lub modyfikacji konfiguracji powinny być logowane.
5.	System OOPZ musi mieć możliwość ochrony przed zmianą konfiguracji przez użytkownika pracującego na stacji końcowej oraz przed odinstalowaniem oprogramowania OOPZ. Wprowadzenie zmian czy deinstalacja powinny być możliwe po wprowadzeniu zdefiniowanego przez Administratora hasła, lub z użyciem innego, bezpiecznego mechanizmu wymuszającego posiadanie specjalnych przywilejów w systemie.
6.	Rozwiązanie musi zapewniać ochronę przed modyfikacją systemu operacyjnego oraz innych zasobów, w tym: a) musi umożliwiać definiowanie reguł pozwalających na blokowanie dostępu do katalogów lub plików, b) musi zapewniać na stacjach roboczych ochronę systemu operacyjnego przed nieuprawnionymi modyfikacjami, korzystając z wbudowanych mechanizmów pozwalających co najmniej na kontrolę: zmian ustawień sieciowych, dodawania programów do obszaru autorun, zmian i tworzenia plików systemowych oraz procesów podszywających się pod procesy systemowe, dodawania nowych usług, zmian kluczowych rejestrów, c) system musi posiadać wbudowane reguły realizujące ochronę kluczowych obszarów stacji roboczej, d) w ramach ochrony przed modyfikacją systemu operacyjnego, musi być możliwe zdefiniowanie procesów, które nie będą podlegały pod tę ochronę.
7.	Musi istnieć możliwość automatycznego instalowania na komputerach roboczych nowych wersji modułów wchodzących w skład OOPZ, poprawek typu service pack oraz hot-fix'ów.
8.	Rozwiązanie musi umożliwiać sprawdzanie adresów, z którymi łączy się stacja robocza w bazie reputacyjnej producenta rozwiązania. W przypadku stwierdzenia próby komunikacji z niebezpiecznym adresem – oprogramowanie winno umożliwiać, co najmniej blokowanie połączenia.
Moduł Antywirusowy (dalej AV)	
9.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu Centralnej Konsoli Zarządzającej obsługującej, co najmniej procesy związane z AV.
10.	System AV musi zapewnić ochronę antywirusową na podstawie następujących mechanizmów: a) plikach definicji antywirusowych (zwanych dalej plikami DEF), b) heurystyki, c) reputacji obiektów z użyciem systemu reputacji producenta.
11.	Pliki z definicjami (sygnatury) – pliki DEF, muszą być regularnie dostarczane przez producenta rozwiązania, oprogramowanie musi pozwalać na, co najmniej dzienne aktualizacje (w okresie trwania wsparcia technicznego). Rozwiązanie musi zapewniać dostęp w czasie rzeczywistym do aktualnych sygnatur zlokalizowanych na serwerach producenta. Oferowane rozwiązanie musi umożliwiać aktualizację plików DEF na stacjach klienckich

	z wykorzystaniem poniższych mechanizmów: a) serwera aktualizacji wskazanego przez producenta, umiejscowionego w Internecie, b) serwera aktualizacji zdefiniowanego przez Zamawiającego, c) serwera aktualizacji umieszczonego w sieci intranetowej Zamawiającego. W przypadku serwera aktualizacji zdefiniowanego przez Zamawiającego lub zlokalizowanego w intranecie Zamawiającego, serwer ten musi umożliwiać zdefiniowanie harmonogramu aktualizacji.
12.	Skanowanie antywirusowe musi odbywać się w dwóch następujących trybach: a) Skanowanie podczas dostępu – skanowanie wybranych plików, gdy jest realizowany dostęp do pliku, b) Skanowanie na żądanie – skanowanie plików według wcześniej zdefiniowanego harmonogramu przez administratora. W przypadku skanowania na żądanie rozwiązanie musi umożliwiać: a) zdefiniowanie skanu, który wykona się według zadanego harmonogramu jednorazowo lub cyklicznie, b) zdefiniowanie skanu, który będzie wstrzymywany w momencie wykrycia podwyższonej aktywności użytkownika na danej stacji roboczej, c) wznawianie skanowania, które zostało wstrzymane w momencie wykrycia pracy użytkownika lub przerwany w wyniku restartu komputera, d) definiowanie obszaru skanowania: wśród dostępnych obszarów powinny być co najmniej: pamięć komputera, wszystkie dyski, wybrane dyski, rejestr systemowy, wszystkie uruchomione procesy, wybrane foldery. W przypadku skanowania podczas uzyskiwania dostępu i skanowania na żądanie rozwiązanie musi umożliwiać: a) definiowanie list plików lub katalogów wykluczonych ze skanowania - zdefiniowane pliki lub lokalizacje będą pomijane przez moduły skanujące, b) włączanie/wyłączanie mechanizmu reputacyjnego plików, c) definiowanie akcji, które będą podjęte przy wykryciu zagrożenia - wśród dostępnych akcji powinny być co najmniej: próba wyczyszczenia pliku, skanowania pliku lub uniemożliwienie dostępu do pliku.
13.	System AV musi zapewnić ochronę przed programami typu Spyware oraz Potencjalnie Niechcianymi Programami.
14.	System AV musi posiadać funkcjonalność lokalnej kwarantanny dla plików zainfekowanych. Uwolnienie plików z kwarantanny powinno być możliwe z użyciem lokalnego interfejsu graficznego, jeśli polityka na to zezwala lub z poziomu Centralnej Konsoli Zarządzającej.
15.	System AV musi mieć możliwość skanowania sektorów rozruchowych dysków.
16.	System AV musi mieć możliwość skanowania dysków sieciowych.
Moduł firewall (dalej FW)	
17.	Moduł FW ma za zadanie kontrolować ruch przychodzący i wychodzący ze stacji roboczej i wymuszać politykę dopuszczonego ruchu wymuszaną przez Administratora.
18.	W ramach modułu FW musi być możliwe tworzenie reguł, które mogą być oparte o: a) kierunek ruchu – wejściowy lub wyjściowy, b) interfejs sieciowy lub sieć logiczna, c) użyty protokół sieciowy, d) typ połączenia sieciowego - powinny być dostępne, co najmniej typy: połączenie przewodowe, połączenie bezprzewodowe,

	e) źródłowych i docelowych adresów IP, f) protokołu obecnego w warstwie czwartej - w przypadku wybrania protokołu TCP oraz UDP możliwość zdefiniowania portu źródłowego i docelowego, g) aplikacji generującej ruch – definicja aplikacji powinna być realizowana poprzez, co najmniej jedną z metod: wskazanie nazwy lub/i ścieżki pliku, skrótu kryptograficznego (hash, minimum jeden z: MD5, SHA-1 lub SHA-2) lub/oraz podpisu cyfrowego pliku.
19.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu Centralnej Konsoli Zarządzającej obsługującej, co najmniej procesy związane z FW.
20.	Wszystkie reguły muszą być zarządzane z poziomu Centralnej Konsoli Zarządzania i rozpatrywane w kolejności wystąpienia.
21.	Wszystkie reguły muszą mieć możliwość logowania wystąpienia danego ruchu i jego przeglądania z poziomu Centralnej Konsoli Zarządzającej.
22.	Musi istnieć możliwość tworzenia reguł przypisanych do konkretnej sieci, wcześniej zdefiniowanej. W przypadku, gdy stacja robocza włącza się do konkretnej sieci, oprócz reguł globalnych, winny obowiązywać reguły przypisane do tej sieci.
23.	Moduł FW musi mieć możliwość izolacji ruchu sieciowego pomiędzy różnymi interfejsami sieciowymi.
24.	W module FW musi istnieć możliwość definiowania, co najmniej sieci zaufanych oraz aplikacji zaufanych by w łatwy sposób zezwalać na ruch sieciowy w obrębie sieci zaufanych lub ruch sieciowy inicjowany przez zaufane aplikacje.
25.	Moduł FW powinien dawać możliwość ograniczania ruchu do/ze stacji roboczej zanim usługi modułu FW będą aktywne.
Moduł ochrony przeglądarek webowych przed złośliwymi stronami web (dalej WP)	
26.	Moduł WP musi współpracować, co najmniej z następującymi przeglądarkami: Microsoft Internet Explorer, Mozilla Firefox i Google Chrome działającymi na stacjach roboczych.
27.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu Centralnej Konsoli Zarządzającej obsługującej co najmniej procesy związane z ochroną ruchu webowego.
28.	Producent modułu WP musi dokładać wszelkich starań, by zapewniać wsparcie dla nowych wersji przeglądarek niedługo po ich ukazaniu się.
29.	Zaproponowane rozwiązanie winno posiadać mechanizm uniemożliwiający wyłączenie ochrony ruchu webowego przez użytkownika na stacji roboczej.
30.	Reputacja stron musi być określana dynamicznie na podstawie reputacyjnej bazy danych udostępnianej przez producenta oprogramowania. Baza reputacyjna winna być regularnie aktualizowana by zapewnić maksymalne bezpieczeństwo ruchu webowego.
31.	W przypadku zidentyfikowania próby dostępu do strony o złej reputacji, mechanizmy aplikacji winny umożliwiać blokowanie dostępu do strony, jednocześnie wyświetlając użytkownikowi stosowny komunikat.
32.	Moduł WP musi posiadać możliwość sprawdzania reputacji obiektów ściągniętych ze strony oraz skanowania ich poprzez przekazanie ich do innych modułów, w tym AV.
33.	Moduł WP musi wykrywać ładowanie stron typu „phishing”, które podszywają się pod inne strony cieszące się dobrym zaufaniem.
34.	Moduł WP musi umożliwiać określenie zakresów blokowanych stron web na podstawie kategorii stron (np. pornografia, hazard, gry, portale społecznościowe, itp.). Musi istnieć możliwość skorzystania, z co najmniej 50 różnych popularnych kategorii utrzymywanych i aktualizowanych przez producenta modułu.
35.	Moduł WP musi umożliwiać blokowanie i przepuszczanie dostępu do wskazanych stron

	web, określonych przez administratora w politykach globalnych, niezależnie od ich poziomu reputacji/ryzyka (tzw. whitelist i blacklist), poprzez podanie adresu DNS lub IP.
36.	Zasady ostrzegania i blokowania dostępu do stron muszą działać także w sytuacji, kiedy stacja robocza pracuje poza siecią firmową Zamawiającego.
Moduł Host IPS (dalej HIPS)	
37.	Oferowane oprogramowanie musi oferować funkcjonalność Host IPS i zapobiegać włamaniom, korzystając z reguł zabezpieczających stację roboczą i uniemożliwiających wykorzystanie podatności aplikacji i systemu operacyjnego.
38.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu Centralnej Konsoli Zarządzającej obsługującej, co najmniej procesy związane z obsługą IPS.
39.	Zaimplementowane mechanizmy IPS muszą operować na sygnaturach znanych ataków i wykorzystywanych przez nie podatności oraz na analizie behawioralnej zachowania procesów działających na chronionych stacjach roboczych.
40.	Oprogramowanie host IPS musi wykrywać i zapobiegać atakom przepełnienia bufora (Buffer Overflow) we wszystkich aplikacjach działających na chronionej stacji roboczej.
41.	Do każdej sygnatury musi być dołączony opis, który opisuje działanie sygnatury i w miarę możliwości odwołuje się do bazy CVE.
42.	Zaoferowane rozwiązanie musi oferować możliwość pisania własnych sygnatur IPS i wysłania ich na chronione systemy.
43.	Oprogramowanie musi uniemożliwiać zmianę konfiguracji IPS przez użytkownika na stacji roboczej.
Moduł kontroli portów (dalej KP)	
44.	Moduł KP musi zapewnić ochronę przed podłączaniem niepożądanych urządzeń do stacji klienckich i powinien być w pełni zarządzany przez co najmniej własną Centralną Konsolę Zarządzającą.
45.	Moduł musi mieć możliwość: logowania zdarzeń, powiadamiania użytkowników o zdarzeniach, blokowania/dopuszczania urządzeń zgodnie z konfiguracją.
46.	Moduł KP musi wykrywać i blokować urządzenia podłączane przez porty zewnętrzne komputera, takie jak pendrive, PDA, kamera cyfrowa, odtwarzacze MP3, drukarki, karty pamięci, aparaty telefoniczne, tablety i inne typy urządzeń oraz umożliwiać zmianę sposobu dostępu do urządzeń posiadających system plików. Moduł KP musi oferować co najmniej poniższe tryby dostępu do urządzeń posiadających system plików: - pełny dostęp, - tylko do odczytu, - blokowanie urządzenia.
47.	Rozwiązanie musi umożliwiać przechowywanie informacji o: nazwie urządzenia, czasie przyłączenia, typie urządzania, kodzie producenta i urządzenia, nr seryjnym i typie systemu plików (zależnie od typu urządzenia i jego zestawu parametrów).
48.	Konfiguracja polityki działania modułu musi umożliwiać zdefiniowanie dopuszczonych do użytkowania zewnętrznych nośników danych USB na podstawie ich numeru seryjnego, ID producenta i ID produktu.
49.	Polityka działania modułu musi umożliwiać przypisanie różnych polityk zależnie od przynależności użytkownika do grup użytkowników synchronizowanych z Active Directory.
Moduł kontroli aplikacji (dalej KA)	
50.	Obsługa konfiguracji, przegląd zdarzeń, itp. winny być obsługiwane z poziomu Centralnej

	Konsoli Zarządzającej obsługującej co najmniej procesy kontroli aplikacji (KA).
51.	System KA musi umożliwiać budowanie whitelist (białych list), czyli list aplikacji dozwolonych na danej stacji roboczej. Aplikacje z tej listy będą mogły być uruchamiane na wskazanych stacjach roboczych.
52.	System KA musi umożliwiać budowanie blacklist (czarnych list), czyli list aplikacji niedozwolonych na danej stacji roboczej. Uruchomienie aplikacji z tej listy musi być blokowane na wskazanych stacjach roboczych.
53.	Rozwiązanie KA ma działać, jako agent na chronionych komputerach w sposób ciągły i reagować natychmiast – nie jest dopuszczalne wykonywanie kontroli aplikacji okresowo, co pewien czas.
54.	Oprogramowanie KA musi być chronione przed nieupoważnionym zatrzymaniem lub odinstalowaniem.
55.	Rozwiązanie musi zapewnić taki sam poziom ochrony niezależnie od tego czy stacja robocza pracuje w sieci firmowej czy poza nią – bez dostępu do CKZ.
56.	Rozwiązanie musi monitorować (generować logi z wystąpienia) i aktywnie blokować próby uruchomienia nieupoważnionego oprogramowania w postaci wykonywalnej (exe, com), skryptów (co najmniej BAT, JavaScript, VBScript), bibliotek, driverów podejmowane przez użytkowników, nieupoważnionych administratorów czy inne oprogramowanie uruchomione na stacji klienckiej.
57.	Rozwiązanie musi zapewniać bazę reputacyjną aplikacji prowadzoną przez producenta oprogramowania. Baza reputacyjna musi umożliwiać określenie poziomu bezpieczeństwa aplikacji. Blokowanie uruchomienia aplikacji musi odbywać się na podstawie zawartości czarnej listy oraz/lub informacji pozyskanych z bazy reputacyjnej. Baza reputacyjna musi być regularnie aktualizowana przeze producenta oprogramowania. Baza reputacyjna musi być dostępna zarówno z sieci wewnętrznej Zamawiającego jak i z Internetu.
58.	Rozwiązanie musi umożliwiać włączenie trybu, w którym przygotowana zostanie automatycznie lista aplikacji uruchomionych na stacji roboczej. Jednocześnie wszystkie umieszczone na tej liście aplikacje otrzymają status „dopuszczonych" do użytkowania na tej stacji. Centralna Konsola Zarządzająca musi umożliwiać przeglądanie list wykrytych i dopuszczonych do działania aplikacji i procesów. CKZ musi również umożliwiać administratorowi zmianę statusu aplikacji umieszczonych na w/w liście na aplikacje blokowane.
59.	Rozwiązanie musi zapewnić obsługę trybu obserwacji/monitorowania, w którym agent realizuje politykę ochrony, ale nie jest wymuszane blokowanie aplikacji. Informacje o blokowaniu, które byłoby podjęte przez agenta KA w normalnym trybie pracy mają być wysyłane do Centralnej Konsoli Zarządzającej celem ułatwienia przygotowania przez administratora docelowej polityki blokowania aplikacji.
60.	Rozwiązanie KA musi umożliwiać wyświetlenie użytkownikowi komunikatu na stacji z informacją o zablokowaniu uruchomienia aplikacji/procesu.
61.	W razie wystąpienia nieautoryzowanej próby uruchomienia aplikacji, procesu, drivera, biblioteki czy skryptu, agent KA ma zapisać informacje o zdarzeniu i przekazać je do Centralnej Konsoli Zarządzającej. W ramach tej informacji powinny się znaleźć, co najmniej następujące dane: a) czas zdarzenia, b) nazwa komputera, na jakim wystąpiło zdarzenie, c) nazwa zalogowanego użytkownika, d) opis zdarzenia z podaniem nazwy aplikacji, procesu, drivera, biblioteki, skryptu, która

	została zablokowana, e) informację o ewentualnym procesie/aplikacji inicjującej zablokowane uruchomienie.
Moduł ochrony poczty elektronicznej (dalej OPE)	
62.	Moduł OPE ma realizować ochronę serwerów poczty elektronicznej pracujących pod kontrolą MS Exchange 2013 i nowszych, wykorzystywanych przez Zamawiającego.
63.	Moduł OPE musi: 1. Zapewniać ochronę przed wszystkimi rodzajami szkodliwego oprogramowania typu: wirus, koń trojański, ransomware, spyware, adware, rootkit, auto-dialer i innymi potencjalnie niebezpiecznymi lub niechcianymi programami. 2. Skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange. 3. Umożliwiać skanowanie bezpośrednio w bazach Exchange na serwerze pocztowym. 4. Umożliwiać usunięcie wiadomości lub załącznika w przypadku wykrycia wirusa lub blokowania wiadomości i wyleczenia / podmiany załącznika na czysty plik zawierający jedynie informację o infekcji. 5. Umożliwiać stosowanie i tworzenie różnych reguł blokowania wiadomości w zależności od zdefiniowanych filtrów/ kryteriów (minimum: nadawca, odbiorca, temat, treść, nazwa i rozszerzenie pliku załącznika, wielkość wiadomości). 6. Posiadać mechanizm antyspamowy wyposażony w co najmniej filtr, sprawdzanie list reputacji, a także kontrolę reputacji poczty. 7. Realizować skanowanie w czasie rzeczywistym otwieranych, zapisywanych plików. 8. Zapewnić skanowanie plików archiwów (spakowanych). 9. Skanować w czasie rzeczywistym pocztę przychodzącą i wychodzącą. 10. Zapewniać skanowanie i oczyszczanie poczty przychodzącej MAPI oraz IMAP w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji klienckiej. W przypadku wykrycia wirusa moduł musi wysłać powiadomienie do administratora systemu pocztowego z użyciem e-mail. 11. Umożliwiać prowadzenie dziennika zdarzeń rejestrującego informacje na temat znalezionych wirusów, dokonanych aktualizacji baz wirusów i wersji oprogramowania, musi mieć możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych modułu. 12. Zapewnić codzienną aktualizację wzorców wirusów. 13. Zapewnić zarządzanie modułem OPE z poziomu Centralnej Konsoli Zarządzania obsługującej przynajmniej konfigurację i kontrolę logów w module OPE.
	Moduł Sandbox
64.	Zaproponowane rozwiązanie musi dawać możliwość konteneryzacji przy wykonywaniu nieznanych plików. Pliki nieznane (z punktu widzenia sygnatur i mechanizmu reputacji) powinny być uruchamiane w izolowanym środowisku (sandbox), które minimalizuje ryzyko wykonania szkodliwej aktywności kodu. Wszystkie dane otrzymywane za pośrednictwem poczty email lub poprzez strony Web, które zostaną przez system uznane za „niepewne” powinny być sprawdzane w izolowanym środowisku. Analiza nie może wymagać przesyłania testowanych plików poza chronioną infrastrukturę. Rozwiązanie winno zapewniać ochronę sieci i innych podsystemów teleinformatycznych przed zaawansowanymi atakami typu APT (Advanced Persistent Threat) mającymi na celu uniknięcie wykrycia przez obecne w infrastrukturze zamawiającego systemy zabezpieczające takie jak bramy e-mail i webowe, systemy IPS/IDS czy oprogramowanie antywirusowe.

	Rozwiązanie winno również ograniczać skutki szkodliwego oprogramowania typu zero-day. Izolowane środowiska (sandbox), w których powinny być sprawdzane podejrzane pliki winny składać się z co najmniej 5 maszyn wirtualnych, które można spreparować w taki sposób, by imitowały stacje robocze użytkowane w infrastrukturze Zamawiającego (te same wersje systemów operacyjnych, charakterystyczne aplikacje, konfiguracja, itp.).

5. Ochrona serwerów fizycznych oraz wirtualnych:

Lp.	Konfiguracja minimalna
1.	System musi zapewniać bezpieczeństwo na poziomie serwerów fizycznych oraz wirtualnych. Moduł ochrony serwerowej musi zapewnić co najmniej poniższe funkcjonalności bezpieczeństwa: firewall, IPS, monitorowanie integralności danych, inspekcja logów, blokowanie ruchu zabronionych aplikacji, anti-malware. Poszczególne funkcjonalności bezpieczeństwa muszą posiadać zakres ochrony co najmniej na poziomie ich odpowiedników na stacjach roboczych, opisanych w części dotyczącej OOPZ. System musi pozwalać na definiowanie polityk bezpieczeństwa przypisanych do konkretnych typów maszyn. Tak utworzone polityki powinny być przypisywane automatycznie (przez system) do nowo tworzonych maszyn, aktywując na nich przewidziane polityką mechanizmy ochrony. W związku z powyższym, system musi umożliwiać tworzenie logicznych grup serwerów. Moduł potrafi ochronić system przed szeregiem znanych podatności, pomimo tego, że system nie posiada zaimplementowanych odpowiednich łatek niwelujących zagrożenie. Moduł działa na zasadzie ochrony przed możliwością wykonania kodu wykorzystującego podatność na podatnej wersji oprogramowania. Moduł ochrony serwerowej winien również na bieżąco analizować zainstalowane aplikacje i w przypadku pojawienia się nowej, automatycznie uruchamiać dodatkowe polityki bezpieczeństwa. Moduł ochrony serwerowej musi zapewniać wsparcie dla następujących systemów operacyjnych: Windows Server 2012/2012R2, Windows Server 2016/2016R2, Windows Server 2019, Ubuntu LTS. Moduł ochrony serwerowej musi zapewniać wsparcie dla środowiska wirtualizacji, co najmniej VMware. System musi pozwalać na swobodny wybór ochrony agentowej lub bezagentowej w przypadku serwerów wirtualnych.

6. Funkcjonalności ogólne:

Lp.	Funkcjonalności ogólne:
1.	**Centralna Konsola Zarządzająca** Rozwiązanie musi dostarczać Centralną Konsolę Zarządzania (dalej zwaną CKZ), która pozwala na zarządzanie z jednego miejsca co najmniej poniższymi modułami: - szyfrowania dysków, - szyfrowania plików, - zarządzania mechanizmami ochrony stacji końcowych przed zagrożeniami (OOPZ). CKZ zapewni funkcjonalność zarządzania politykami w celu konfiguracji oraz implementacji ustawień modułów na poziomie samych modułów oraz poziomie stacji roboczych. Konsola zarządzająca CKZ zapewni pojedynczy punkt monitoringu dla oprogramowania

	anti-malware, oraz modułów badających zawartość danych pod kątem bezpieczeństwa. CKZ umożliwia administratorom systemów monitorowanie i raportowanie aktywności takich jak: infekcje, naruszenia bezpieczeństwa oraz punkty wejścia w przypadku wirusów oraz malware. Funkcjonalności CKZ pozwolą administratorom systemów ściągnąć i zastosować uaktualnienia komponentów poprzez sieć, dzięki czemu zapewniona zostanie aktualność oraz konsystencja systemu. CKZ umożliwi manualne oraz predefiniowane aktualizacje. CKZ umożliwi także konfigurowanie oraz administrowanie produktami w grupach lub osobno. CKZ służy do wymiany informacji o zagrożeniach w obrębie organizacji, w której zainstalowane są komponenty wchodzące w skład obsługiwanych modułów. Centralna Konsola Zarządzania musi się składać z oprogramowania serwerowego oraz agentów instalowanych na stacjach końcowych, których zadaniem jest konfigurowanie zarządzanych produktów oraz zbieranie zdarzeń i przekazywanie ich do CKZ. Zarządzanie wszystkimi modułami i pełnym zakresem funkcji dostarczonego systemu ochrony musi następować z jednej i tej samej aplikacji (konsoli) działającej co najmniej na serwerze Microsoft Windows (wymagane wsparcie dla co najmniej wersji Windows Server 2012, Windows Server 2012 R2, Windows Server 2016/2016 R2, Windows Server 2019) lub Linux i korzystającej z bazy danych Microsoft SQL (wymagane wsparcie co najmniej dla wersji SQL 2014) lub bazy danych MySQL co najmniej w wersji 5.5. CKZ musi być skalowalna i umożliwiać zarządzanie co najmniej 1 tysiącem komputerów i zainstalowanych na nich produktów - wymaganie dotyczy możliwości technicznych, wydajnościowych aplikacji a nie możliwości jakie dają zaoferowane licencje. Centralna konsola zarządzająca (CKZ) musi umożliwić zdalną instalację produktów na komputerach z domeny Microsoft Active Directory objętych ochroną, bez konieczności stosowania dodatkowych narzędzi i oprogramowania, z możliwością zaplanowania z wyprzedzeniem momentu wykonania instalacji dla poszczególnych komputerów i grup komputerów. Centralna konsola zarządzająca (CKZ) musi umożliwiać tworzenie szczegółowych konfiguracji pracy poszczególnych produktów i dystrybucję polityk oraz wymuszanie ich zastosowania. CKZ musi posiadać możliwość powiadamiania o wszystkich zdarzeniach za pomocą poczty elektronicznej, wiadomości SNMP i syslog lub wywołania komendy/skryptu. CKZ musi mieć możliwość integracji z Active Directory zarówno w rozumieniu powielenia struktury komputerów jak i autentykacji administratorów i dynamicznego przypisywania uprawnień w serwerze zarządzającym w zależności od przynależności do odpowiedniej grupy w Active Directory. CKZ musi być przygotowana do pracy w strefie DMZ (dostępnej z sieci publicznych) tak, aby było możliwe zarządzanie komputerami znajdującymi się poza siecią korporacyjną, bez zestawiania połączeń VPN lub SSL VPN i aby jednocześnie podstawowy serwer zarządzający zawierający CKZ nie był narażony na potencjalne ataki z zewnątrz. System zarządzania CKZ ma zapewnić centralne repozytorium (oparte na relacyjnej bazie danych) dla logów i zdarzeń logowanych przez wszystkie moduły systemu ochrony: a) Zbieranie zdarzeń logowanych we wszystkich modułach dostarczanego systemu ochrony na wszystkich chronionych węzłach (komputerach i serwerach) i składowanie ich w centralnym repozytorium będącym integralną częścią systemu. b) Zbieranie zdarzeń musi obejmować wszystkie zdarzenia logowane przez moduły dostarczonego oprogramowania.

	c) Mechanizm zbierania zdarzeń musi umożliwiać ograniczenie zbieranych zdarzeń na podstawie wybieranego przez administratora kryterium, d) Podsystem zbierający zdarzenia musi zapewniać centralne zarządzanie z pojedynczej konsoli dla wszystkich komponentów oprogramowania. Konsola zarządzająca CKZ ma umożliwiać centralne opracowanie raportów na podstawie zgromadzonych danych i prezentację ich w różnych formatach (np. PDF, XML, HTML): a) Raporty powinny być generowane na żądanie, ale powinna istnieć możliwość określenia zakresu raportu i częstotliwości jego automatycznego generowania b) Raporty powinny bazować na predefiniowanych przez producenta szablonach dla poszczególnych zarządzanych produktów, a także powinna być możliwość tworzenia własnych raportów przez administratorów. CKZ musi posiadać dostępny bez dodatkowych opłat licencyjnych interfejs API umożliwiający Zamawiającemu automatyzację podstawowych czynności administracyjnych - w tym co najmniej: dodawanie i usuwanie kont administratorów systemu, usuwanie logów, uruchamianie i zatrzymywanie zadań do wykonania przez serwer zarządzający (np. ściągaj aktualizację produktów), przypisywanie określonych polityk produktów do grup komputerów, dodawanie komputerów do listy zarządzanych maszyn wraz z automatycznym uruchomieniem dla nich zadań instalacji oprogramowania ochronnego, usuwanie komputerów z listy zarządzanych maszyn.

W przypadku zaoferowania rozwiązania równoważnego Wykonawca zapewni wdrożenie, migrację danych z systemu posiadanego przez Zamawiającego, wsparcie techniczne na czas trwania umowy oraz szkolenie 5 administratorów w wymiarze 40 (czterdziestu) godzin.