**Załącznik E**

**do SIWZ Wzory dokumentów**

**Minimalne wymagania funkcjonalne oprogramowania**

**(*dotyczy zamówienia podstawowego oraz opcji)***

**Opis minimalnych wymagań funkcjonalnych dla oprogramowania antywirusowego** dla Infrastruktury Wirtualizacyjnej VMware vSphere with Operation Management Enterprise Plus Edition opartej o oprogramowanie Trend Micro Deep Security Manager w funkcjonalności AntiMalware oraz Web Reputation posiadane przez Zamawiającego zawarty został poniżej. Zamawiający wymaga aby oprogramowanie:

1. Dostarczone przez Wykonawcę Oprogramowanie antywirusowe w ramach zamówienia podstawowego i prawa opcji wraz z 36 miesięczną gwarancją producenta pozwalające na rozbudowę posiadanych klastrów wirtualizacyjnych, pracujących w infrastrukturze Zamawiającego pod kontrolą posiadanego oprogramowania „VMware vSphere with Operation Management Enterprise Plus Edition” w wersji 6.x chronionych systemem antywirusowym Deep Security Manager w funkcjonalności AntiMalware oraz Web Reputation, poprzez zalicencjonowanie kolejnych serwerów fizycznych dodanych do tych klastrów Oprogramowaniem antywirusowym, bez utraty posiadanych funkcjonalności.

2. Wszystkie komponenty, na których będzie zainstalowane Oprogramowanie antywirusowe muszą być zainstalowane jako maszyny wirtualne pracujące w środowisku VMware vSphere with Operation Management Enterprise Plus Edition” w wersji 6.x Zamawiającego. Wykonawca jest zobowiązany do dostarczenia wszystkich licencji (włącznie z licencjami na systemy operacyjne dla nowych komponentów oraz dodatkowe oprogramowanie), niezbędnych do prawidłowego działania Oprogramowania.

3. Licencjonowanie Oprogramowania, ze względu na dynamicznie rozwijającą się infrastrukturę Zamawiającego, musi być oparte na bazie liczby fizycznych procesorów chronionego hosta (licencjonowanie per socket).

4. Wymagania Zamawiającego dotyczące Zarządzania infrastrukturą Systemu AV:

4.1 Pełna administracja konfiguracją oraz monitorowanie środowiska maszyn wirtualnych za pomocą centralnej konsoli administracyjnej posiadanej przez Zamawiającego, w pełnej wymaganej przez Zamawiającego funkcjonalności (centralna instalacja, konfiguracja, zarządzanie, raportowanie i administrowanie oprogramowaniem), w szczególności:

a) Dostępna funkcjonalność określenia harmonogramu oraz wymuszenia skanowania na żądanie,

b) Określenie reakcji w przypadku wykrycia wirusa,

c) Dostępna funkcjonalność określenia obszarów skanowania, typów skanowanych katalogów, plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych obszarów,

d) Dostępna funkcjonalność zdefiniowania harmonogramu lub częstotliwości pobierania aktualizacji wirusów od producenta/producentów,

e) Dostępna funkcjonalność zarządzania zdarzeniami i raportowanie – natychmiastowe alarmowanie aktywności wirusów w administrowanej sieci,

f) Dostępna funkcjonalność prezentacji informacji o poziomie bezpieczeństwa na centralnej konsoli zarządzającej systemami,

g) Dostępna funkcjonalność tworzenia kont dla administratorów o różnych stopniach uprawnień dla różnych komputerów lub grup komputerów oraz różnych produktów.

5.Wymagania Zamawiającego na Oprogramowanie Antywirusowe w zakresie funkcjonalności AntiMalware i Web Reputation (AM / WR):

5.1 Dostarczone Oprogramowanie musi posiadać następujące funkcjonalności:

a) Bezagentowa ochrona maszyn wirtualnych w obrębie serwera hosta bez względu na ich stan (aktywne, uśpione, przywrócone do poprzedniego stanu, sklonowane) realizowana w przypadku wszystkich opisanych poniżej funkcjonalności,

b) Zapewnia ochronę niewspieranych przez ich producentów systemów operacyjnych oraz aplikacji działających na maszynach wirtualnych,

c) Oprogramowanie antywirusowe musi zapewniać „bezagentową” ochronę dla serwerów i desktopów wirtualnych,

d) Oprogramowanie musi pozwalać na określenie obszarów skanowania, typów skanowanych plików oraz na wykluczenie ze skanowania określonych obszarów dla skanowania w czasie rzeczywistym, ręcznego skanowania oraz skanowania określonego w harmonogramie,

e) Oprogramowanie musi umożliwiać określenie harmonogramu skanowania (obiekty i grupy), oraz wymuszenia skanowania w danej chwili,

f) Oprogramowanie musi opierać się na mechanizmie skanowania nowych bądź zmienionych plików w celu skrócenia czasu skanowania oraz zwiększenia wydajności,

g) Oprogramowanie musi posiadać heurystyczną technologię do wykrywania nowych, nieznanych wirusów,

h) Oprogramowanie musi posiadać funkcjonalność zdefiniowania harmonogramu lub częstotliwości pobierania aktualizacji bazy wirusów, wszelkich poprawek oprogramowania oraz umożliwiać określenie centralnego punktu dystrybucji uaktualnień i poprawek oprogramowania w infrastrukturze Zamawiającego,

i) Oprogramowanie musi pozwalać na określenie reakcji w przypadku wykrycia wirusa (czyszczenie, automatyczne usunięcie, kwarantanna), oraz na natychmiastowe raportowanie o zdarzeniach (e-mail, wiadomości SNMP),

j) Oprogramowanie musi realizować funkcję hierarchii i delegacji uprawnień administratorów, zarówno dla grup jak i poszczególnych obiektów,

k) Zarządzanie Oprogramowaniem musi odbywać się poprzez standardową przeglądarkę WWW i połączenie https (z wykluczeniem SSL 3.0, 2.0, 1.0), która nie wymaga instalacji żadnych dodatkowych komponentów, umożliwiając dostęp do konsoli na kilku stacjach jednocześnie lub dedykowaną konsolę w technologii Grubego Klienta,

l) Oprogramowanie musi posiadać funkcjonalność wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „greyware”, „adware”, „keylogger”, „dialer”, „trojan”, „antimalware”,

m) Oprogramowanie musi posiadać możliwość blokowania połączeń do adresów URL określonych przez producenta systemu, jako niebezpieczne, również w przypadku, gdy połączenia są nawiązywane przez procesy działające na chronionych serwerach,

n) Oprogramowanie musi mieć możliwość konfiguracji lokalnego serwera reputacji plików, synchronizującego się z chmurą producenta, który umożliwiał będzie weryfikację reputacji plików i adresów URL bez konieczności łączenia się z Internetem,

o) Oprogramowanie musi mieć możliwość zdefiniowania statycznych list adresów URL, do których połączenia będą zawsze blokowane przez system,

p) Oprogramowanie musi mieć możliwość tworzenia logicznych grup serwerów w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa,

q) Oprogramowanie musi umożliwiać ochronę maszyn znajdujących się w strefie DMZ,

r) Oprogramowanie musi mieć możliwość generowania i wysyłania raportów w wybranym formacie ( minimum pdf),

s) Oprogramowanie musi posiadać funkcjonalność przekazywania zdarzeń o zagrożeniach do centralnego serwera lub systemu typu SIEM. W przypadku wysyłanie informacji o zdarzeniach do systemu SIEM administrator musi mieć możliwość zdefiniowania centralnego systemu SIEM lub odrębnych systemów dla każdej z polityk, grup chronionych serwerów lub pojedynczych serwerów,

t) Serwer zarządzający oprogramowania musi posiadać w pełni udokumentowane API pozwalające na jego integrację z zewnętrznymi systemami zarządzającymi firm trzecich,

u) Oprogramowanie musi mieć możliwość tworzenia ról administratorów i przydzielania uprawnień co najmniej w zakresie:

v) Serwerów lub grup serwerów

w) Polityk lub grup polityk

x) Poszczególnych funkcjonalności systemu,

y) Oprogramowanie musi mieć możliwość tworzenia drzewa polityk zależnych, w którym polityki pochodne dziedziczą ustawienia od polityk na wyższym poziomie. Administratorzy posiadający uprawnienia jedynie do polityk pochodnych nie mogą mieć możliwości wprowadzania zmian do ustawień dziedziczonych.

6. Wymagania Zamawiającego na Oprogramowanie Antywirusowe w zakresie funkcjonalności Integrity Monitoring i Log Inspection (IM / LI):

6.1 Dostarczone oprogramowanie musi posiadać następujące funkcjonalności:

a) System musi pozwalać na monitorowanie wskazanych plików, katalogów, serwisów, wpisów w rejestrach oraz procesów i informowanie o wprowadzanych zmianach w oparciu o zdefiniowane kryteria.

b) W przypadku serwerów wirtualnych działających pod kontrolą systemu Windows system musi posiadać możliwość realizowania monitorowania wskazanych plików, katalogów oraz wpisów w rejestrach i informowanie o wprowadzanych zmianach w oparciu o zdefiniowane kryteria bez konieczności instalowania dedykowanego agenta na wskazanym, chronionym serwerze.

c) Informacja o wprowadzonych zmianach musi zawierać co najmniej nazwę użytkownika lub procesu, który wprowadził zmianę, nazwę pliku lub wpisu w rejestrze, w którym została wprowadzona zmiana, datę i czas wprowadzenia zmiany, nazwę serwera na którym została wprowadzona zmiana, oraz nazwę reguły oraz która została wykorzystana

d) System musi posiadać predefiniowany zestaw reguły dostarczonych przez producenta określających wskazane do monitorowania pliki wpisy w rejestrach oraz monitorowane serwisy, w zależności od chronionego systemu lub aplikacji.

e) System musi posiadać możliwość ręcznego zdefiniowania przez administratora monitorowanych plików oraz wpisów w rejestrach.

f) System musi posiadać możliwość zdefiniowania wykluczeń plików znajdujących się w monitorowanym katalogu.

g) System musi posiadać możliwość monitorowania hypervisora i informowania o wprowadzanych w nim zmianach.

h) System musi posiadać reguły dostarczone przez producenta określające wskazane do zbierania i analizy logi, w zależności od chronionego systemu

i) System musi posiadać możliwość automatycznego uruchamiania odpowiednich reguł niezależnie dla każdego chronionego serwera, w zależności od systemu operacyjnego lub aplikacji.

j) System musi posiadać możliwość tworzenia polityk stanowiących zbiór reguł dostarczonych przez producenta oraz zdefiniowanych przez administratora

k) System musi posiadać możliwość tworzenia drzew polityk, w których polityki położona na niższych gałęziach dziedziczą ustawienia z polityk położonych na gałęziach wyższych

l) System musi posiadać możliwość tworzenia granularnych ról administratorów z możliwością definiowania uprawnień z dokładnością do pojedynczej polityki lub serwera.

m) System musi posiadać możliwość automatycznego przypisywania polityk w oparciu o algorytmy zdefiniowane przez administratora, co najmniej w przypadku utworzenia nowego serwera wirtualnego, jego przeniesienia

n) Algorytmy w oparciu, o które system przydziela polityki muszą pozwalać na zdefiniowanie automatycznych działań, co najmniej w zależności od nazwy serwera, systemu operacyjnego oraz nazwy wykorzystywanego serwera zarządzającego.

o) Wszystkie funkcjonalności systemu muszą być zarządzane z pojedynczej konsoli, tej samej, która jest wykorzystywana do zarządzania funkcjonalnościami AntiMalware i Web Reputation.

7. Wymagania Zamawiającego na Oprogramowanie Antywirusowe w zakresie funkcjonalności Intrusion Detection and Prevention i Firewall (IPS / FW):

7.1 Dostarczone oprogramowanie musi posiadać następujące funkcjonalności:

a) System musi posiadać możliwość kontroli oraz blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.

b) System musi posiadać predefiniowaną bazę najpopularniejszych aplikacji oraz komunikatorów (włączając w to gadu-gadu i skype)

c) System musi posiadać możliwość heurystycznego wykrywania transmisji na podstawie częstotliwości jej występowania oraz zdefiniowanego zakresu portów.

d) System musi posiadać możliwość przełączania pomiędzy trybem blokowania ruchu i trybem detekcji zdarzeń w sposób globalny dla wszystkich reguł.

e) System musi posiadać moduł umożliwiający blokowanie transmisji na podstawie zdefiniowanej charakterystyki ruchu na podstawie sygnatury oraz zdefiniowanego ciągu znaków (patternu).

f) System musi pozwalać na sprawdzanie w czasie rzeczywistym poziomu bezpieczeństwa nieznanych aplikacji poprzez zapytania przesyłane poprzez siec do systemu serwerów producenta.

g) System musi posiadać możliwość ochrony podatności systemów i aplikacji, bez konieczności instalowania poprawek dostarczanych przez producentów tych systemów oraz aplikacji.

h) System musi posiadać dwukierunkowy stanowy firewall (stateful firewall) pozwalający na łatwą izolacje interfejsów i nie wymagający restartów systemu.

i) System musi pełni wspierać IPv6.

j) System musi umożliwiać kontrolę połączeń wychodzących i przychodzących w komunikacji sieciowej z możliwością kontroli niestandardowych portów TCP (możliwość zdefiniowania na podstawie numeru protokołu oraz numeru typu ramki).

k) System musi posiadać możliwość przełączenia trybu działania reguł firewalla z trybu blokowania ruchu w tryb detekcji zdarzeń.

l) Wszystkie funkcjonalności powinny być dostarczane bezagentowo.

m) System musi posiadać umiejętność pracy ze zdeformowanymi pakietami, brakującymi flagami itp. Anomaliami.

n) System powinien umożliwiać definiowanie trybu pracy Tap oraz Inline dla każdego chronionego obiektu i polityki bezpieczeństwa.

o) System powinien umożliwiać inspekcję HTTPS bez potrzeby wykorzystywania dodatkowych rozwiązań.

p) System musi wykorzystywać mechanizmy pseudo-stanowe (pseudo-stateful) dla protokołów bezstanowych (UDP, ICMP).

8. Integracja dostarczanego w ramach niniejszego postępowania oprogramowania antywirusowego ze środowiskiem posiadanym przez Zamawiającego musi być możliwa w zakresie:

9. zarządzania i konfigurowania z jednej wspólnej centralnej konsoli zarządzającej (Trend Micro Deep Security Manager), w pełnej wymaganej przez Zamawiającego funkcjonalności;

a. współpracy z usługą katalogową i systemem poczty elektronicznej posiadanymi przez Zamawiającego;

b. definiowania poziomów uprawnień użytkowników administracyjnych systemu wirtualizującego na podstawie przynależności do grup w usłudze katalogowej Zamawiającego;

c. centralnej konsoli zarządzającej dla wszystkich serwerów hypervisora już będących w posiadaniu Zamawiającego i serwerów objętych licencjami dostarczanymi w ramach niniejszego postępowania oraz dla wszystkich maszyn wirtualnych zlokalizowanych na nowo dostarczanej infrastrukturze i pracujących na dotychczasowym środowisku Zamawiającego;

d. Współpracy z systemem backupowym posiadanym przez Zamawiającego;

e. jednorodnych ról administracyjnych i poziomów uprawnień użytkowników.

10. Polityka licencjonowania oprogramowania do wirtualizacji nie może wiązać licencji w żaden sposób ze środowiskiem sprzętowym.

11. Oprogramowanie musi umożliwiać uruchomienie ochrony antywirusowej na serwerach fizycznych o łącznej liczbie od 1-8 procesorów w zależności od zamówienia Zamawiającego, niezależnie od ilości maszyn wirtualnych znajdujących się na pojedynczym serwerze