

Załącznik nr 1 do SIWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (SOPZ)

I. Zamówienie podstawowe

1. Licencja typ A – umożliwiająca zabezpieczenie 240 urządzeń końcowych

Nazwa licencji	Opis wymagań technicznych – równoważnych
<p>Licencje typu Fortigate Endpoint Telemetry & Compliance lub równoważne</p>	<ol style="list-style-type: none"> 1. Licencja musi być kompatybilna z posiadanym przez Zamawiającego systemem zabezpieczeń sieciowych składającym się z 2 urządzeń Fortigate 500 D pracujących w klastrze HA <p>Licencja umożliwiająca:</p> <ol style="list-style-type: none"> 2. Sprawdzanie stanu hosta co najmniej w zakresie zainstalowanego oprogramowania antywirusowego dla systemów Windows 7 i 10 3. Przesyłanie logów do posiadanego przez Zamawiającego serwera Fortianalyzer dla systemów Windows 7 i 10 oraz Mac OS X 4. W przypadku niespełniania przez hosta warunków, możliwość podjęcia następujących akcji: blokowanie hosta, ostrzeżenie o niespełnianiu wymagań, automatyczna aktualizacja ustawień w celu spełnienia wymagań dla systemów Windows 7 i 10 oraz Mac OS X 5. Sprawdzenia stanu hosta pod względem podatności. W przypadku wykrycia podatności o określonym poziomie musi być możliwość ustawienia kwarantanny dla hosta. Wymagane jest obsługiwane następujących poziomów podatności: Krytyczny, Wysoki, Średni, Niski i Informacyjny dla systemów Windows 7 i 10 oraz Mac OS X 6. Definiowanie minimalnych wymagań dla oferowanego oprogramowania co najmniej w zakresie: <ol style="list-style-type: none"> a. profilu filtrowania sieci Web dla systemów Windows 7 i 10 oraz Mac OS X, b. profilu kontroli aplikacji dla systemów Windows 7 i 10 oraz Mac OS X, c. minimalnej wersji oferowanego oprogramowania dla systemów Windows 7 i 10 oraz Mac OS X 7. Połączenie IPSec VPN i SSL VPN z posiadanym przez Zamawiającego systemem zabezpieczeń sieciowych Fortigate 500 D dla systemów Windows 7 i 10 oraz Mac OS X.

2. Licencja typ B – umożliwiająca zabezpieczenie 240 urządzeń końcowych

Nazwa licencji	Opis wymagań technicznych – równoważnych
Licencje typu Forticlient EMS lub równoważne	<ol style="list-style-type: none"> 1. Licencja musi być kompatybilna z posiadanym przez Zamawiającego systemem zabezpieczeń sieciowych składającym się z 2 urządzeń Fortigate 500 D pracujących w klastrze HA 2. Licencje muszą zawierać prawo do instalacji serwera zarządzającego oferowanym oprogramowaniem <p>Licencja umożliwiająca:</p> <ol style="list-style-type: none"> 3. zdalne zarządzanie oferowanym oprogramowaniem zainstalowanym na systemach Windows 7 i 10 4. lokalizację urządzenia z zainstalowanym oferowanym oprogramowaniem na systemie Windows 7 i 10 oraz Mac OS X 5. Przesyłanie logów do posiadanego przez Zamawiającego serwera Fortianalyzer dla systemów Windows 7 i 10 oraz Mac OS X 6. Integracje z Windows Active Directory w zakresie pozwalającym wykorzystywać grupy użytkowników do określania profili filtrowania sieci Web i kontroli aplikacji w oferowanym oprogramowaniu zainstalowanym na systemach Windows 7 i 10 oraz Mac OS X 7. Aktualizację oferowanego oprogramowania zainstalowanego na systemach Windows 7 i 10 oraz Mac OS X 8. Skanowanie hosta pod kątem obecności znanych podatności dla systemów Windows 7 i 10 oraz Mac OS X 9. Ustawianie i wymuszanie (użytkownik końcowy nie może zmienić ustawień) profili bezpieczeństwa w oferowanym oprogramowaniu zainstalowanym na systemach Windows 7 i 10 oraz Mac OS X. 10. Połączenie IPSec VPN i SSL VPN z posiadanym przez Zamawiającego systemem zabezpieczeń sieciowych Fortigate 500 D dla systemów Windows 7 i 10 oraz Mac OS X

II. Prawo opcji

1. Licencja typ A – umożliwiająca zabezpieczenie maksymalnie 100 urządzeń końcowych

Nazwa licencji	Opis wymagań technicznych – równoważnych
Licencje typu Fortigate Endpoint Telemetry & Compliance lub równoważne	<ol style="list-style-type: none"> 1. Licencja musi być kompatybilna z posiadanym przez Zamawiającego systemem zabezpieczeń sieciowych składającym się z 2 urządzeń Fortigate 500 D pracujących w klastrze HA <p>Licencja umożliwiająca:</p> <ol style="list-style-type: none"> 2. Sprawdzanie stanu hosta co najmniej w zakresie zainstalowanego oprogramowania antywirusowego dla systemów Windows 7 i 10

	<ol style="list-style-type: none"> 3. Przesyłanie logów do posiadanego przez Zamawiającego serwera Fortianalyzer dla systemów Windows 7 i 10 oraz Mac OS X 4. W przypadku niespełniania przez hosta warunków, możliwość podjęcia następujących akcji: blokowание hosta, ostrzeżenie o niespełnianiu wymagań, automatyczna aktualizacja ustawień w celu spełnienia wymagań dla systemów Windows 7 i 10 oraz Mac OS X 5. Sprawdzenia stanu hosta pod względem podatności. W przypadku wykrycia podatności o określonym poziomie musi być możliwość ustawienia kwarantanny dla hosta. Wymagane jest obsługiwanie następujących poziomów podatności: Krytyczny, Wysoki, Średni, Niski i Informacyjny dla systemów Windows 7 i 10 oraz Mac OS X 6. Definiowanie minimalnych wymagań dla oferowanego oprogramowania co najmniej w zakresie: <ol style="list-style-type: none"> a. profilu filtrowania sieci Web dla systemów Windows 7 i 10 oraz Mac OS X, b. profilu kontroli aplikacji dla systemów Windows 7 i 10 oraz Mac OS X, c. minimalnej wersji oferowanego oprogramowania dla systemów Windows 7 i 10 oraz Mac OS X 7. Połączenie IPSec VPN i SSL VPN z posiadanym przez Zamawiającego systemem zabezpieczeń sieciowych Fortigate 500 D dla systemów Windows 7 i 10 oraz Mac OS X.
--	---

2. Licencja typ B – umożliwiająca zabezpieczenie maksymalnie 100 urządzeń końcowych

Nazwa licencji	Opis wymagań technicznych – równoważnych
Licencje typu Forticlient EMS lub równoważne	<ol style="list-style-type: none"> 1. Licencja musi być kompatybilna z posiadanym przez Zamawiającego systemem zabezpieczeń sieciowych składającym się z 2 urządzeń Fortigate 500 D pracujących w klastrze HA 2. Licencje muszą zawierać prawo do instalacji serwera zarządzającego oferowanym oprogramowaniem <p>Licencja umożliwiająca:</p> <ol style="list-style-type: none"> 3. zdalne zarządzanie oferowanym oprogramowaniem zainstalowanym na systemach Windows 7 i 10 4. lokalizację urządzenia z zainstalowanym oferowanym oprogramowaniem na systemie Windows 7 i 10 oraz Mac OS X 5. Przesyłanie logów do posiadanego przez Zamawiającego serwera Fortianalyzer dla systemów Windows 7 i 10 oraz Mac OS X 6. Integracje z Windows Active Directory w zakresie pozwalającym wykorzystywać grupy użytkowników do

	<p>określania profili filtrowania sieci Web i kontroli aplikacji w oferowanym oprogramowaniu zainstalowanym na systemach Windows 7 i 10 oraz Mac OS X</p> <ol style="list-style-type: none">7. Aktualizację oferowanego oprogramowania zainstalowanego na systemach Windows 7 i 10 oraz Mac OS X8. Skanowanie hosta pod kątem obecności znanych podatności dla systemów Windows 7 i 10 oraz Mac OS X9. Ustawianie i wymuszanie (użytkownik końcowy nie może zmienić ustawień) profili bezpieczeństwa w oferowanym oprogramowaniu zainstalowanym na systemach Windows 7 i 10 oraz Mac OS X.10. Połączenie IPSec VPN i SSL VPN z posiadanym przez Zamawiającego systemem zabezpieczeń sieciowych Fortigate 500 D dla systemów Windows 7 i 10 oraz Mac OS X
--	---