

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup i wdrożenie centralnego systemu ochrony urządzeń końcowych dla PGL LP

Przedmiotem zamówienia jest zakup i wdrożenie w Państwowym Gospodarstwie Leśnym Lasy Państwowe (PGL LP), centralnego systemu zabezpieczającego przed zagrożeniami komputerowymi z funkcjonalnością EDR (ang. Endpoint Detection and Response), wraz ze wsparciem serwisowym przez cały okres umowy, do obsługi komputerów klasy PC, komputerów klasy serwerowej, urządzeń mobilnych, zarówno w sieci WAN (kilkaset odległych lokalizacji połączonych siecią IP VPN) jak i w sieci Internet.

I. Słownik

Ileć w postanowieniach niniejszego Opisu Przedmiotu Zamówienia (OPZ) zostały użyte pojęcia i definicje wymienione poniżej, nadaje się im następujące znaczenie:

1. System AV – rozwiązanie służące do ochrony stacji roboczych oraz serwerów i urządzeń mobilnych przed zagrożeniami komputerowymi, zagrożeniami sieciowymi oraz identyfikacji nietypowych zachowań i naruszeń bezpieczeństwa sieci w ramach ochrony urządzeń końcowych.
2. Administrator centralny – zdefiniowana w Systemie AV rola administratora definiującego profile konfiguracyjne, role użytkowników i administratorów oraz inne parametry Systemu AV. Administrator centralny posiada wgląd do zasobów Systemu AV we wszystkich jednostkach organizacyjnych PGL LP. Rola upoważnia do zgłaszania awarii, awarii krytycznych i defektów SZBiM do Wykonawcy.
3. Administrator regionalny - zdefiniowana w Systemie AV rola administratora przypisująca profile konfiguracyjne, role administratorów jednostki organizacyjnej PGL LP oraz inne parametry Systemu AV dla konkretnych użytkowników. Administrator regionalny posiada wgląd do zasobów Systemu AV w jednostce własnej oraz w jednostkach podległych.
4. Administrator jednostki organizacyjnej PGL LP - zdefiniowana w Systemie AV rola administratora przypisująca profile konfiguracyjne, oraz inne parametry Systemu AV dla konkretnych użytkowników końcowych i urządzeń. Administrator jednostki posiada wgląd wyłącznie do zasobów administrowanej jednostki.
5. Architektura Systemu AV – podział oprogramowania na komponenty oraz definicje funkcji tych komponentów oraz występujące między nimi relacje.
6. Awaria – zgłoszona dysfunkcyjność Systemu AV mająca wpływ na działanie oprogramowania, usług i funkcjonalności Systemu AV określonych w wymaganiach OPZ.
7. Awaria krytyczna – zgłoszona dysfunkcja Systemu AV polegająca na jego działaniu niezgodne z opisanym w aktualnej dokumentacji, które powoduje zawieszanie się pracy Systemu AV, wprowadza niespójność w bazie danych lub zaburzenia w integralności

danych; sytuacja, w której System AV w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcji w systemie. Awarią krytyczną jest także sytuacja, kiedy wyżej wymienione zdarzenia spowodowane są błędem uniemożliwiającym współpracę Systemu AV z systemem operacyjnym lub z bazą danych. Awarią krytyczną jest również podatność w Systemie AV mogąca zagrozić poufności bądź integralności danych Klienta.

8. Defekty – inne zgłoszone dysfunkcjonalności Systemu AV nie mające istotnego wpływu na działanie oprogramowania, usług i funkcjonalności Systemu AV określonych w wymaganiach OPZ.
9. DMZ – wydzielony obszar sieci komputerowej PGL LP nienależący ani do sieci wewnętrznej, ani do sieci publicznej.
10. Konsola (operatorska/zarządzająca) Systemu AV – Wbudowane w System AV narzędzie umożliwiające administrowanie Systemem AV za pośrednictwem przeglądarki internetowej lub dedykowanej aplikacji instalowanej na komputerach administratorów.
11. PGL LP - oznacza Państwowe Gospodarstwo Leśne Lasy Państwowe.
12. Profil konfiguracyjny – zestaw ujednoliconych ustawień definiowanych przez administratora.
13. Urządzenia klasy PC – urządzenie pracujące pod kontrolą systemu operacyjnego Microsoft Windows 10 i nowszych, Red Hat Enterprise Linux 6 i nowszych, Debian 10 i nowszych, działające na urządzeniu fizycznym.
14. Urządzenia klasy serwerowej – urządzenie pracujące pod kontrolą systemu operacyjnego Microsoft Windows Server 2012 R2 i nowszych, Red Hat Enterprise Linux 6 i nowszych, Debian 10 i nowszych, działające na urządzeniu fizycznym lub platformie wirtualizacyjnej (VMware, Microsoft Hyper-V).
15. Urządzenie mobilne - urządzenie przenośne pracujące pod kontrolą systemu Google Android 8 i nowsze lub Apple IOS 10 i nowsze lub iPad OS 13 i nowsze.
16. SSL/TLS – protokół zapewniający poufność i integralność transmisji danych, a także uwierzytelnienie serwera oraz klienta.
17. SZBiM – System Zgłaszania Błędów i Modyfikacji funkcjonujący w PGL LP, służący do komunikacji między użytkownikami i Wykonawcą oraz rejestracji i obsługi zgłoszeń awarii przez użytkowników.
18. Użytkownik – pracownik PGL LP, korzystający z Systemu AV.
19. Wysoka dostępność usługi (HA, High Availability) – dostępność serwera zarządzającego Systemu AV na poziomie 99,99% czasu.
20. Zgłoszenie – informacja przekazana do Wykonawcy o zaistniałym defekcie, awarii lub awarii krytycznej poprzez SZBiM lub telefonicznie, potwierdzona zwrotnie przez e-mail od Wykonawcy.

II. Specyfikacja zamawianego oprogramowania

LP	Wymagania	Minimalne	Opcjonalne (dodatkowo punktowane w kryteriach oceny ofert)
1.	Wymagania dla architektury Systemu AV		
1.1	<p>Komponenty Systemu AV mogą być zainstalowane w infrastrukturze PGL LP (Vmware, Microsoft Windows Serwer 2016, Red Hat Enterprise Linux 6) lub korzystać z rozwiązania chmurowego producenta. Zamawiający dopuszcza rozwiązanie hybrydowe. Zamawiający dopuszcza rozwiązanie chmurowe wyłącznie dla konsoli zarządzającej urządzeniami znajdującymi się poza siecią WAN LP, które łączą się z wykorzystaniem publicznej sieci Internet. Dla serwerów i urządzeń stacjonarnych znajdujących się na stałe w sieci WAN LP wymagana jest konsola zainstalowana w infrastrukturze LP.</p> <p>Platforma sprzętowa/wirtualna przeznaczona na oprogramowanie serwerowe (serwer/serwery centralne):</p> <ul style="list-style-type: none"> - vCPU 16 CORE , RAM 96GB , dysk 400GB. <p>Wykonawca jest zobowiązany dostarczyć wszystkie wymagane licencje w tym licencję na bazę danych konieczną do wdrożenia systemu zgodnie z OPZ na posiadanej przez Zamawiającego platformie wirtualizacyjnej VMware z zastrzeżeniem jak poniżej.</p> <p>Zamawiający informuję, że posiada licencję Windows Server 2016 Data Center obejmującą przydzielone zasoby sprzętowe. Jeżeli dostarczane rozwiązanie wymaga instalacji systemu operacyjnego Windows Server 2016 to nie ma konieczności dostawy przez Wykonawcę takiej licencji, ponieważ posiadana licencji obejmuje wszystkie maszyny wirtualne na przydzielonych zasobach sprzętowych.</p> <p>Wykonawca musi wziąć pod uwagę warunki dostarczanych licencji i dostarczyć licencję dla wdrażanego systemu w środowisku Zamawiającego składającego się z platformy wirtualizacyjnej VMware. Przeznaczone do</p>	TAK	

	wdrożenia DataCenter składa się z 6 serwerów ESXi po dwa CPU każdy, w sumie 12 CPU.		
1.2	Komponenty zarządzające Systemu AV zainstalowane w infrastrukturze PGL LP muszą pracować w trybie wysokiej dostępności (HA) i posiadać redundantne elementy w obu centrach przetwarzania danych PGL LP - podstawowym i zapasowym. Zamawiający zapewni Load Balancer, który zrównoważy obciążenie na wszystkich serwerach i zagwarantuje ciągłość dostarczanych usług. Całkowity brak komunikacji z drugim centrum przetwarzania danych nie może wpływać na funkcjonalność rozwiązania (wszystkie usługi muszą być dostępne). Po powrocie komunikacji z drugim centrum przetwarzania danych systemy muszą się zsynchronizować i przejść ponownie w tryb HA.	TAK	
1.3	Komponenty zarządzające Systemu AV zainstalowane w infrastrukturze PGL LP służące do komunikacji z urządzeniami końcowymi pracującymi w publicznej sieci Internet muszą mieć możliwość odseparowania ich do strefy DMZ.	TAK	
1.4	Dla urzędów pracujących w sieci WAN (IP VPN) serwer aktualizacji baz zagrożeń musi być dostępny z sieci WAN (IP VPN).	TAK	
1.5	System AV musi obsłużyć minimum 54 000 urzędów w tym 26 000 urzędów mobilnych, 26 000 urzędów klasy PC i 2 000 urzędów klasy serwerowej bez konieczności jego rozbudowy.	TAK	
1.6	Wdrażany System AV musi zawierać wszystkie niezbędne licencje na dostarczone oprogramowanie oraz funkcjonalności określone w wymaganiach OPZ, w tym licencję na ochronę urzędów końcowych oraz licencje niezbędne do wdrożenia dostarczanego Systemu AV .	TAK	
1.7	Wszystkie licencje muszą pochodzić z oficjalnych kanałów dystrybucji producentów. Licencje muszą być wolne od wad prawnych i fizycznych.	TAK	
2.	Wymagania ogólne dla Systemu AV		
2.1	System AV musi oferować pomoc oraz instrukcję obsługi w języku polskim. Wykonawca zapewni wsparcie techniczne w języku polskim.	TAK	
2.2	System AV chroniący urządzenia końcowe musi oferować interfejs w języku polskim.	TAK	
2.3	System AV musi oferować pełne wsparcie i wymaganą przez OPZ funkcjonalność dla systemów operacyjnych zainstalowanych na urządzeniach klasy PC, serwerach fizycznych i	TAK	

	wirtualnych (VMware, Hyper-v) oraz urządzeń mobilnych.		
2.4	System AV chroniący urządzenia mobilne musi współdziałać z VMware Workspace ONE wykorzystywanym w PGL LP, we wszystkich możliwych trybach rejestracji urządzenia w VMware Workspace ONE.	TAK	
3	Wymagania dotyczące integracji z systemami PGL LP		
3.1	System AV musi umożliwiać synchronizację z usługami katalogowymi Microsoft Active Directory w wersji Windows Server 2012 R2 i nowszej. Integracja Systemu AV z AD musi umożliwiać pobranie z usługi katalogowej bazy użytkowników, grup domenowych oraz komputerów i przypisanie ich do hierarchicznej struktury w konsoli zarządzającej Systemu AV, odzwierciedlającej strukturę organizacyjną PGL LP na podstawie których budowane będą polityki oraz reguł bezpieczeństwa.	TAK	
3.2	System AV musi umożliwić hierarchiczne zarządzanie urządzeniami na trzech poziomach: centralnym, regionalnym i jednostki. Dostęp do wszystkich urządzeń tylko dla administratorów centralnych, dostęp do urządzeń z regionu tylko dla administratorów swojego regionu oraz dostęp dla administratorów jednostki tylko dla urządzeń z swojej jednostki.	TAK	
3.3	Wykonawca zapewni integrację Systemu AV z posiadany przez PGL LP systemem SPLUNK.	TAK	
4	Wymagania dotyczące centralnego zarządzania Systemem AV		
4.1	System AV musi posiadać centralną infrastrukturę zarządzania pracującą w trybie wysokiej dostępności usługi (HA, High Availability), którą administrator zarządza poprzez konsolę zarządzającą.	TAK	
4.2	Konsola zarządzająca musi oferować interfejs w języku polskim lub w języku angielskim.	TAK	
4.3	Konsola zarządzająca musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej lub dedykowaną aplikację.	TAK	
4.4	Dostęp do konsoli zarządzającej musi odbywać się przy pomocy poświadczeń kont użytkowników z Active Directory oraz lokalnych kont administracyjnych.	TAK	
4.5	Konsola zarządzająca musi umożliwiać równoczesny dostęp dla min. 500 administratorów.	TAK	
4.6	Konsola zarządzająca musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych i serwerów na poziomie jednostki organizacyjnej.	TAK	

4.7	System AV oferuje możliwość automatycznej instalacji na urządzeniach końcowych pracujących pod kontrolą systemu Windows.		TAK
4.8	System AV oferuje możliwość wysyłania komunikatów na pojedyncze urządzenie, grupę urządzeń.		TAK
4.9	System AV musi oferować możliwość utworzenia zadania dla pojedynczego urządzenia, grupy urządzeń oraz wszystkich urządzeń.	TAK	
4.10	System AV musi mieć możliwość tworzenia statycznych i dynamicznych grup urządzeń na podstawie filtrów.	TAK	
4.11	System AV musi oferować możliwość utworzenia własnych raportów i skorzystanie z predefiniowanych wzorów. Jeżeli do tworzenia własnych raportów konieczne jest dodatkowe oprogramowanie to należy je dostarczyć wraz wymaganą licencją.	TAK	
4.12	System AV musi oferować możliwość wygenerowania raportu na żądanie i zgodnie z harmonogramem.	TAK	
4.13	System AV musi mieć możliwość generowania raportów okresowych i wysyłania ich za pomocą wiadomości e-mail.	TAK	
4.14	System AV musi oferować możliwość tworzenia własnych treści powiadomień o zdarzeniach lub skorzystania z predefiniowanych wzorów.	TAK	
4.15	System AV musi posiadać możliwość zarządzania własnymi licencjami na poziomie jednostki organizacyjnej PGL LP.	TAK	
4.16	System AV umożliwia wykorzystanie własnego certyfikatu SSL do komunikacji z konsolą zarządzającą.		TAK
5.	Wymagania dotyczące ochrony dla komputerów i serwerów z systemem Windows		
5.1	W pełni działająca ochrona w czasie rzeczywistym.	TAK	
5.2	Skanowanie dysków lokalnych, nośników wymiennych oraz dysków sieciowych.	TAK	
5.3	Skanowanie plików w trakcie operacji ich otwierania, tworzenia oraz wykonywania.	TAK	
5.4	Skanowanie sektorów startowych i systemu UEFI.	TAK	
5.5	Skanowanie z wykorzystaniem heurystyki.	TAK	
5.6	Ochrona przed szkodliwym oprogramowaniem.	TAK	
5.7	Ochrona przed niepożądanymi aplikacjami (zawierającymi reklamy, instalującymi niechciane dodatki do przeglądarek).	TAK	
5.8	Ochrona przed szkodliwymi aplikacjami skompresowanymi za pomocą programów pakujących.	TAK	
5.9	Ochrona przed potencjalnie niebezpiecznymi programami z kategorii: odnajdywanie kluczy	TAK	

	produktu, generatory kluczy licencyjnych, narzędzia do hackowania, programy do łamania haseł, keylogery.		
5.10	Możliwość włączenia skanowania wstępnego zaraz po zainstalowaniu aplikacji do ochrony urządzenia.	TAK	
5.11	Ochrona przed ukrywającymi się aplikacjami typu rootkit.	TAK	
5.12	Możliwość skanowania skryptów powershell oraz Windows Script Host.	TAK	
5.13	Ochrona sieci komputerowej z wykorzystaniem zaporę firewall.	TAK	
5.14	Kontrola ruchu sieciowego wychodzącego i przychodzącego do urządzenia.	TAK	
5.15	Możliwość tworzenia profili zaporę firewall i przypisywanie ich do interfejsów sieciowych.	TAK	
5.16	Wykrywanie modyfikacji aplikacji dla której zdefiniowano wcześniej regułę w zaporze firewall.	TAK	
5.17	Blokowanie dostępu do Internetu na poziomie aplikacji oraz adresacji sieciowej.	TAK	
5.18	Ochrona IDS przed zagrożeniami z sieci.	TAK	
5.19	Tworzenie własnych reguł IDS	TAK	
5.20	Ochrona przed sieciami typu botnet.	TAK	
5.21	Ochrona przed sieciowymi atakami typu brute force.	TAK	
5.22	Tworzenie własnych reguł przed atakami typu brute force.	TAK	
5.23	Wykrywanie włamań na protokoły SMB, RPC oraz RDP.	TAK	
5.24	Ochrona przed skanowaniem portów.	TAK	
5.25	Ochrona stron internetowych, poczty email, aplikacji pod względem zagrożeń komputerowych.	TAK	
5.26	Blokowanie stron internetowych wg kategorii.	TAK	
5.27	Blokowanie domen internetowych, adresów IP z lokalnych oraz internetowych czarnych list		TAK
5.28	Ochrona połączeń szyfrowanych dla stron internetowych.		TAK
5.29	Ochrona dokumentów pakietów biurowych pod względem zagrożeń komputerowych.	TAK	
5.30	Skanowanie antywirusowe wg harmonogramu i na żądanie.	TAK	
5.31	Skanowanie antywirusowe pełne i wg zdefiniowanego zakresu.	TAK	
5.32	Skanowanie antywirusowe wskazanego elementu w menu kontekstowym.	TAK	
5.33	Skanowanie podłączanych nośników danych typu pendrive, dysk USB, karta pamięci na żądanie lub automatycznie po ich podłączeniu.	TAK	
5.34	Skanowanie plików skompresowanych i kontenerów typu: zip, rar, 7-zip, iso, itp.	TAK	

5.35	Możliwość ustawienia poziomu zagnieżdżenia archiwów oraz maksymalnego rozmiaru skanowanego archiwum.	TAK	
5.36	Korzystanie z reputacji obiektów bazujących np. na wskaźnikach włamania IoC np. adresy IP, domeny, skróty plików złośliwego oprogramowania wprowadzanych: ręcznie, automatycznie importowanych z pliku, zewnętrznego źródła np. z chmury producenta.	TAK	
5.37	Ochrona Systemu AV przed niepożądaną (nieautoryzowaną) modyfikacją, usunięciem, wyłączeniem.	TAK	
5.38	Wymuszenie uruchomienia ochrony antywirusowej przy starcie systemu.	TAK	
5.39	Wyłączenie ochrony antywirusowej na określony czas poprzez podanie hasła lub przez administratora urządzenia.	TAK	
5.40	Instalacja lub usunięcie programu antywirusowego wymaga uprawnień administratora urządzenia.	TAK	
5.41	Aktualizacja baz zagrożeń wg harmonogramu lub na żądanie.	TAK	
5.42	Możliwość definiowania profili aktualizacji baz zagrożeń.	TAK	
5.43	Definiowanie wykluczeń przed skanowaniem i ochroną lub dodanie do elementów zaufanych na poziomie plików, katalogów, aplikacji, adresów IP, adresów sieci, domen internetowych.	TAK	
5.44	Obsługa blokowania dostępu do podłączanych urządzeń USB również za pośrednictwem stacji dokującej i HUBów USB.	TAK	
5.45	System AV powinien umożliwiać kontrolowanie podłączanych urządzeń USB. Kontrola powinna polegać na analizie czy urządzenie USB znajduje się na liście jako dopuszczone do użytkowania (biała lista). Urządzenia spoza listy powinny być blokowane.	TAK	
5.46	Lista dopuszczonych urządzeń USB musi funkcjonować oraz być zarządzana przez administratorów na poziomie jednostki organizacyjnej.	TAK	
5.47	System AV musi umożliwiać eksport i import listy dozwolonych urządzeń USB (biała lista) jak i niedozwolonych urządzeń USB (czarna lista).	TAK	
5.48	System AV powinien umożliwiać tworzenie reguł odczytu/zapisu na wskazanych urządzeniach USB.	TAK	
5.49	Narzędzie do ręcznego odinstalowywania Systemu AV z chronionych urządzeń.	TAK	
5.50	Powiadamianie użytkownika w formie komunikatu o wystąpieniu zagrożenia.	TAK	

5.51	Powiadomienie administratora urządzenia o wystąpieniu zagrożenia. Stan widoczny w konsoli zarządzającej, opcjonalnie wysłanie wiadomości email.	TAK	
5.52	Ręczna wysyłka próbki wirusa do producenta w celu analizy.	TAK	
5.53	Znalezione zainfekowane obiekty powinny móc zostać przeniesione do kwarantanny w celu późniejszej analizy.	TAK	
5.54	Dane statystyczne zbierane i wysyłane przez system antywirusowy do producenta muszą być zanonimizowane.	TAK	
6	Wymagania dla ochrony dla komputerów i serwerów z systemem Linux		
6.1	W pełni działająca ochrona w czasie rzeczywistym.	TAK	
6.2	Skanowanie dysków lokalnych, nośników wymiennych oraz dysków sieciowych.	TAK	
6.3	Skanowanie plików w trakcie operacji ich otwierania, tworzenia oraz wykonywania.	TAK	
6.4	Skanowanie sektorów startowych i systemu UEFI.	TAK	
6.5	Skanowanie z wykorzystaniem heurystyki.	TAK	
6.6	Ochrona przed szkodliwym oprogramowaniem.	TAK	
6.7	Skanowanie antywirusowe wg harmonogramu i na żądanie.	TAK	
6.8	Skanowanie antywirusowe pełne i wg zdefiniowanego zakresu.	TAK	
6.9	Skanowanie plików skompresowanych i kontenerów typu: zip, rar, 7-zip, iso, itp.	TAK	
6.10	Możliwość ustawienia poziomu zagnieżdżenia archiwów oraz maksymalnego rozmiaru skanowanego archiwum.	TAK	
7	Wymagania dla ochrony dla urządzeń mobilnych		
7.1	Instalacja Systemu AV na urządzeniu mobilnym musi być możliwa poprzez domyślny sklep z aplikacjami dostępny na urządzeniu.	TAK	
7.2	Rejestracja Systemu AV na urządzeniu mobilnym musi skutkować pojawieniem się zarejestrowanego urządzenia w konsoli zarządzającej w grupie urządzeń przypisanej do jednostki organizacyjnej w strukturze PGL LP, do której należy użytkownik Systemu AV.	TAK	
7.3	W pełni działająca ochrona w czasie rzeczywistym.	TAK	
7.4	Ochrona przed szkodliwym oprogramowaniem..	TAK	
7.5	Skanowanie antywirusowe wg harmonogramu i na żądanie.	TAK	
7.6	Ochrona przed niepożądanymi aplikacjami mającymi wpływ na wydajność i niezawodność urządzenia.	TAK	
7.7	Ochrona przed potencjalnie niebezpiecznymi programami z kategorii: programy do łamania haseł, keylogery.	TAK	

7.8	Skanowanie antywirusowe pełne i wg zdefiniowanego zakresu.	TAK	
7.9	Powiadamianie administratora o złamaniu zabezpieczeń urządzenia typu rooted lub Jailbreak.		TAK
7.10	Generowanie listy zainstalowanych aplikacji.	TAK	
7.11	Widoczna w konsoli zarządzającej informacja o parametrach urządzenia jak model, wersja oprogramowania itp.	TAK	
7.12	Blokowanie instalowania aplikacji z poza innych źródeł niż domyślny sklep z aplikacjami dostępny na urządzeniu.	TAK	
7.13	Powiadamianie użytkownika w formie komunikatu o wystąpieniu zagrożenia .	TAK	
7.14	Funkcja ochrony urządzenia po zgubieniu, kradzieży.	TAK	
7.15	Wyświetlanie informacji kontaktowych po zablokowaniu zgubionego, skradzionego urządzenia.	TAK	
7.16	Wysyłanie poleceń przy pomocy SMS umożliwiające blokowanie, odblokowywanie urządzenia, przywracanie ustawień fabrycznych i kasowanie danych.	TAK	
7.17	Blokowanie aplikacji.	TAK	
7.18	Możliwość zdefiniowania listy wyjątków nie blokowanych aplikacji.	TAK	
8	Wymagania dla funkcjonalności EDR		
8.1	Detekcja znanych oraz nieznanymi zagrożeń w oparciu o analizę zachowania elementów systemu operacyjnego/procesów/aplikacji polegające na korelowaniu ich w incydenty i odpowiednie priorytetowanie (ocena ryzyka, segmentacja alertów). Ochrona powinna wykorzystywać najnowocześniejsze mechanizmy, w tym algorytmy uczenia maszynowego, sztucznej inteligencji, korelację przepływów sieciowych.	TAK	
8.2	Identyfikacja zagrożeń APT (ang. Advanced Persistent Threads) i ataków ukierunkowanych.	TAK	
8.3	Wizualizacja zagrożeń w celu szybszego wykrycia przyczyny infekcji złośliwym oprogramowaniem.	TAK	
8.4	Możliwość wykonywania poleceń Powershell na urządzeniach chronionych z systemem Microsoft Windows.	TAK	
8.5	Przeszukiwanie incydentów i zebranych danych z urządzeń chronionych pod kątem wektorów ataków.	TAK	
8.6	Reakcja na zdiagnozowane zagrożenia: - powiadomienie innych urządzeń o zagrożeniu, - usunięcie pliku, - usunięcie lub modyfikacja klucza rejestru, - zakończenie procesu,	TAK	

	- wyłączenie interfejsu sieciowego, - wyłączenie urządzenia.		
8.7	Wykrywanie i blokowanie użycia klientów sieci Torrent, przeglądarek TOR, klientów VPN.	TAK	
8.8	Współpraca z bazą MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK).	TAK	
8.9	W przypadku wykrycia zagrożenia system przedstawi działania naprawcze.	TAK	
8.10	Okres przechowywania zdarzeń dot. wykrytych zagrożeń: co najmniej 1 rok.	TAK	
8.11	Okres przechowywania wszystkich zdarzeń z chronionych urządzeń: co najmniej 1 miesiąc.	TAK	

III. Wymagania dotyczące szkoleń administratorów

1. Szkolenia powinny być podzielone na dwa poziomy: administratorów centralnych (maksymalnie 10 osób) oraz administratorów regionalnych (maksymalnie 50 osób). W szkoleniu dla administratorów regionalnych uczestniczyć będą również administratorzy centralni.
2. Szkolenia powinny być zrealizowane w siedzibie Zamawiającego lub jednym z ośrodków szkoleniowych PGL LP na terenie RP, - w zależności od sytuacji epidemiologicznej szkolenie za zgodą stron może zostać zrealizowane w formie zdalnej.
3. Szkolenia powinny odbyć się w terminach uzgodnionych z Zamawiającym, z co najmniej dwutygodniowym wyprzedzeniem.
4. Pierwsze szkolenie administratorów centralnych przeprowadzone powinno być nie później niż 14 dni od pozytywnego odbioru centralnego Systemu AV, na działającej infrastrukturze zamawiającego.
5. Pierwsze szkolenie administratorów regionalnych, powinno odbyć się po zakończonych szkoleniach administratorów centralnych, ale nie później niż 30 dni od pozytywnego odbioru centralnego Systemu AV.
6. Szkolenia powinny być przeprowadzone co najmniej w dwóch terminach dla każdego z poziomów.
7. Szkolenia powinny zajmować nie mniej niż 16h dla każdego poziomu, nie więcej niż 8h w jednym dniu.
8. Szkolenia przeprowadzone mają być w języku polskim przez osobę posiadającą certyfikat dla oferowanego rozwiązania wystawiony przez Producenta rozwiązania potwierdzający znajomość systemu na poziomie co najmniej zaawansowanym.
9. Szkolenia dla administratorów centralnych powinny obejmować zakresem sposób realizacji funkcjonalności Systemu AV, wskazanych w OPZ w najwyższym stopniu uprawnień w szczególności:
instalację/deinstalację Systemu AV w środowisku serwerowym, tworzenie kopii i przywracania całego środowiska z Systemem AV w przypadku awarii, przełączanie przetwarzania pomiędzy ośrodkami danych, szczegółową obsługę

konsoli zarządzającej i integrację z AD, aktualizacje Systemu AV do wyższych wersji (dotyczy również klientów), aktualizacje bazy wirusów w Systemie AV i ich dystrybucja na urządzenia, dystrybucja oprogramowania na urządzenia końcowe, dodawanie i przypisywanie uprawnień administratorom regionalnym i jednostek, , tworzenie grup urządzeń, tworzenie i stosowanie polityk na urządzeniach, zapisywanie i odtwarzanie schematów ustawień, zarządzanie licencjami.

10. Szkolenia dla administratorów regionalnych powinny obejmować zakresem co najmniej: szczegółową obsługę konsoli zarządzającej i integrację z AD, dodawanie i przypisywanie uprawnień administratorom jednostek organizacyjnych, , tworzenie i stosowanie polityk na urządzeniach, zapisywanie i odtwarzanie schematów ustawień, zarządzanie licencjami, instalację/deinstalację klientów, aktualizacje, tworzenie instalatorów, tworzenie zadań, generowanie raportów i powiadomień, rozpoznawanie zagrożeń i podejmowanie właściwych działań.
11. Materiały szkoleniowe powinny być przygotowane przez Wykonawcę na platformę e-learning w formacie umożliwiającym zaimportowanie na platformę Moodle wykorzystywaną przez PGL LP.
12. Materiały szkoleniowe powinny obejmować swoim zakresem co najmniej tematy poruszane na szkoleniach administratorów, w tym Wykonawca zobowiązuje się do:
 - 1) dostarczenia instrukcji instalacji agentów i konfiguracji klientów,
 - 2) dostarczenia instrukcji generowania pakietów instalacyjnych klientów,
 - 3) wszystkie materiały powinny być w języku polskim.

IV. Rodzaj licencji

1. Wykonawca powinien dostarczyć licencje na oferowane rozwiązanie w tym wszystkie niezbędne licencje do działania Systemu AV.
2. Wszystkie dostarczone licencje powinny być objęte wsparciem producenta, co najmniej przez okres trwania Umowy, liczony od daty dostarczenia licencji.
3. Powinny one być podzielone na urządzenia mobilne oraz klasy PC/serwerowej chyba, że są to licencje uniwersalne, a ich koszt jest jednakowy.
4. W przypadku użycia licencji na urządzeniu mobilnym pod kontrolą systemu WorkspaceOne w trybie rejestracji COPE, powinna zostać wykorzystana jedna licencja (lub więcej, pod warunkiem kosztu równego jednej licencji).
5. Ochrona urządzeń końcowych powinna być licencjonowana na użytkownika lub na urządzenie.
6. Licencje powinny być przenaszalne pomiędzy użytkownikami i urządzeniami danego typu.
7. Oferowany System AV musi umożliwiać zakup pojedynczej licencji na użytkownika lub urządzenie końcowe.
8. Licencja na użytkownika powinna być rozumiana jako licencja na komputer oraz na urządzenie mobilne. Ilość pracowników w PGL LP wynosi ok. 26 000 osób.

V. Wymagania gwarancyjne i serwisowe.

1. System AV musi być objęty 48 miesięcznym wsparciem technicznym producenta.
2. System AV musi być objęty 48 miesięcznym wsparciem technicznym Wykonawcy, świadczonym w dni robocze w godzinach 6:00-18:00. Przyjmowanie i obsługa zgłoszeń będzie realizowana w języku polskim.
3. Cząsy reakcji serwisu zostały opisane poniżej:

Opis	Czas reakcji	Wstępne rozwiązanie problemu przywrócenie funkcjonalności	Ostateczne rozwiązanie problemu
Awarie krytyczne (Poziom 1)	1 godz.	4 godz.	24 godz.
Awarie (Poziom 2)	2 godz.	8 godz.	5 dni roboczych
Defekty (Poziom 3)	8 godz.	3 dni robocze	Rozwiązanie problemu w uzgodnionym czasie nie dłuższym niż 30 dni roboczych

Powyższe czasy liczone są od momentu przekazania zgłoszenia do Wykonawcy.

4. W okresie wsparcia wymagany jest zapewnienie dostępu dla Zamawiającego do wszystkich najnowszych wersji oprogramowania, poprawek, itp. oraz stron technicznych producenta.