URZĄD GMINY CIECHANÓW

ul. Fabryczna 8, 06-400 Ciechanów
tel.: 23 6722646, 23 6722210, 23 6723876, 23 6722646 email: urzad@gminaciechanow.pl

Załącznik nr 1 do Zapytania ofertowego/
Załącznik nr 1 do Umowy nr .../.../2024

Opis Przedmiotu Zamówienia

1. Przedmiotem zamówienia jest dostawa **50 szt.** (40 szt. dla Urzędu Gminy Ciechanów i 10 szt. dla GOPS Ciechanów) licencji na oprogramowanie **ESET PROTECT Elite** lub dostawa licencji na oprogramowanie równoważne na okres **24 miesięcy**.
2. Oznaczenie przedmiotu zamówienia wg Kod CPV:
   48760000-3 Pakiety oprogramowania do ochrony antywirusowej
   48000000-8 Pakiety oprogramowania i systemy informatyczne
   72611000-6 Usługi w zakresie wsparcia technicznego
3. Zamawiający posiada licencje ESET PROTECT Entry ON-PREM:
   3.1. Liczba chronionych stacji roboczych, urządzeń mobilnych i serwerów: **41 szt.** (31 szt. w Urzędzie Gminy Ciechanów i 10 szt. w GOPS Ciechanów).
   3.2. Licencja ważna do: **2024-06-28**.
   3.3. Identyfikator publiczny: 333-KTU-JTX.
4. Licencje na oprogramowanie zabezpieczające przed złośliwym oprogramowaniem, zostaną dostarczone w terminie 3 dni roboczych od daty zawarcia umowy.
5. Licencja na Oprogramowanie zostanie udzielona w terminie 3 dni roboczych od dnia podpisania Umowy, nie wcześniej niż **2024-06-28**, na **24 miesiące**.
6. Wykonawca dostarczy dokumenty licencyjne, warunki licencjonowania oraz klucze licencyjne i instrukcje instalacji do Oprogramowania na adres e-mail: admin@gminaciechanow.pl.
7. Udzielona na oprogramowanie licencja musi umożliwiać co najmniej:
   7.1. Dostęp do subskrypcji aktualnych baz sygnatur.
   7.2. Dostęp do najnowszej wersji oprogramowania.
   7.3. Wsparcia technicznego producenta lub dystrybutora oprogramowania.
8. Parametry i funkcjonalności dostarczonego oprogramowania, nie mogą być gorsze niż wskazane poniżej:

8.1. Administracja zdalna w chmurze

8.1.1. Serwer administracyjny musi być dostępny w chmurze producenta oprogramowania antywirusowego.
8.1.2. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia przechowywanych danych.
8.1.3. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
8.1.4. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
8.1.5. Serwer Administracyjny musi obsługiwać przynajmniej 50 000 stacji roboczych/serwerów.
8.1.6. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.

8.1.7. Serwer administracyjny musi posiadać wsparcie dla „VDI” oraz „Golden Master Image”.
8.1.8. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
8.1.9. Administrator musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
8.1.10. Administrator musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap.
8.1.11. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.
8.1.12. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
8.1.13. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
8.1.14. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
8.1.15. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania.
8.1.16. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
8.1.17. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.
8.1.18. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.
8.1.19. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
8.1.20. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8.1.21. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami,

raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.

8.1.22. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.

8.1.23. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie generowania raportów i usuwania stacji roboczych. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.

8.1.24. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.

8.1.25. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.

8.1.26. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.

8.1.27. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.

8.1.28. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

8.1.29. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.

8.1.30. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.

8.1.31. Szablon grupy dynamicznej musi umożliwiać zdefiniowane przedziału czasowego kiedy grupa dynamiczna ma działać.

8.1.32. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.

8.1.33. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.

8.1.34. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.

8.1.35. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.

8.1.36. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.

8.1.37. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.

8.1.38. Serwer administracyjny musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
8.1.39. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
8.1.40. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
8.1.41. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
8.1.42. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.
8.1.43. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
8.1.44. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.
8.1.45. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF i CSV.
8.1.46. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
8.1.47. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
8.1.48. Powiadomienia mailowe mają być wysyłane w formacie HTML.
8.1.49. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.
8.1.50. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email.
8.1.51. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
8.1.52. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
8.1.53. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
8.1.54. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
8.1.55. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
8.1.56. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

8.1.57. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
8.1.58. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.
8.1.59. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.
8.1.60. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.
8.1.61. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.
8.1.62. Serwer musi wspierać wysyłanie logów do systemu SYSLOG.
8.1.63. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych.
8.1.64. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.
8.1.65. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).
8.1.66. Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.

8.2. Ochrona stacji roboczych - Windows

8.2.67. Rozwiązanie musi wspierać systemy Windows 10/Windows 11.
8.2.68. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
8.2.69. Rozwiązanie musi wspierać architekturę ARM64.
8.2.70. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
8.2.71. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
8.2.72. Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim.
8.2.73. Skuteczność rozwiązania potwierdzona nagrodami VB100 i AV-comparatives. Ochrona antywirusowa i antyspyware
8.2.74. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
8.2.75. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
8.2.76. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
8.2.77. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
8.2.78. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.
8.2.79. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

8.2.80. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
8.2.81. Rozwiązanie musi posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
8.2.82. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
8.2.83. Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
8.2.84. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
8.2.85. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.
8.2.86. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
8.2.87. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
8.2.88. Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
8.2.89. Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
8.2.90. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
8.2.91. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
8.2.92. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
8.2.93. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
8.2.94. Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
8.2.95. Rozwiązanie musi posiadać wbudowany konektor dla programu Microsoft Outlook.
8.2.96. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu Microsoft Outlook.
8.2.97. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

8.2.98. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
8.2.99. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
8.2.100. Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
8.2.101. Rozwiązanie musi posiadać możliwość blokowania możliwości przeglądania wybranych stron internetowych. Rozwiązanie musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
8.2.102. Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
8.2.103. Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
8.2.104. Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
8.2.105. Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
8.2.106. Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
8.2.107. Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego.
8.2.108. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
8.2.109. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
8.2.110. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
8.2.111. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
8.2.112. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne –jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
8.2.113. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
8.2.114. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.

8.2.115. Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
8.2.116. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
8.2.117. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
8.2.118. Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło.
8.2.119. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo.
8.2.120. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
8.2.121. Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
8.2.122. Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
8.2.123. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
8.2.124. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
8.2.125. Rozwiązanie musi posiadać umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
8.2.126. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
8.2.127. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
8.2.128. Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
8.2.129. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.

8.2.130. W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
8.2.131. Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
8.2.132. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).
8.2.133. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
- tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
- tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
- tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
- tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

8.2.134. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
8.2.135. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
8.2.136. Rozwiązanie musi posiadać zaawansowany skaner pamięci.
8.2.137. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
8.2.138. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
8.2.139. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
8.2.140. Rozwiązanie musi posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
8.2.141. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
8.2.142. Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.

8.2.143. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji.
8.2.144. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
8.2.145. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
8.2.146. Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
8.2.147. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
8.2.148. Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
8.2.149. W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania.
8.2.150. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
8.2.151. Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
8.2.152. Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
8.2.153. Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
8.2.154. Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie.
8.2.155. W trakcie instalacji rozwiązanie ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM.
8.2.156. W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
8.2.157. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej.
8.2.158. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
8.2.159. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
8.2.160. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.

8.2.161. Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
8.2.162. Rozwiązanie musi posiadać możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
8.2.163. Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
8.2.164. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
8.2.165. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
8.2.166. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
8.2.167. Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
8.2.168. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
8.2.169. Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”
8.2.170. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
8.2.171. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
8.2.172. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
8.2.173. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
8.2.174. Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet.
8.2.175. Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB.
8.2.176. Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
8.2.177. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.

8.3. Ochrona przed spamem

8.3.178. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
8.3.179. Rozwiązanie musi umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.

8.3.180. Rozwiązanie musi umożliwiać automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
8.3.181. Rozwiązanie musi posiadać możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
8.3.182. Rozwiązanie musi posiadać możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
8.3.183. Rozwiązanie musi posiadać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
8.3.184. Rozwiązanie musi możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
8.3.185. Rozwiązanie musi domyślnie współpracować z folderem „Wiadomości-śmieci", dostępnym w programie Microsoft Outlook.
8.3.186. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana"
8.3.187. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana".
8.3.188. Rozwiązanie musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

8.4. Zapora osobista (personal firewall)

8.4.189. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
- tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
- tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
- tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
- tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

8.4.190. Rozwiązanie musi oceniać reguły zapory systemu Windows.
8.4.191. Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych.
8.4.192. Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
8.4.193. Rozwiązanie musi posiadać możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
8.4.194. Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
8.4.195. Rozwiązanie musi posiadać możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
8.4.196. Rozwiązanie musi posiadać możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
8.4.197. Rozwiązanie musi wykrywać modyfikację w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.

8.4.198. Rozwiązanie musi posiadać możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
8.4.199. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
8.4.200. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
8.4.201. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
8.4.202. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
8.4.203. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
8.4.204. Rozwiązanie musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów:
- z aplikacją lokalną, którą administrator wskazuje z listy,
- z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP. Kontrola dostępu do stron internetowych
8.4.205. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
8.4.206. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
8.4.207. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
8.4.208. Podstawowe kategorie, w jakie rozwiązanie musi być wyposażone to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
8.4.209. Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych.
8.4.210. Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta.
8.4.211. Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
8.4.212. Rozwiązanie musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj.

8.4.213. Rozwiązanie musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.

8.5. Bezpieczna przeglądarka

8.5.214. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.

8.5.215. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

8.5.216. Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki.

8.5.217. Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę.

8.5.218. Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki.

8.5.219. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

8.6. Sandbox w chmurze

8.6.220. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

8.6.221. Rozwiązanie musi wykorzystywać do działania chmurę producenta.

8.6.222. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.

8.6.223. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.

8.6.224. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.

8.6.225. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.

8.6.226. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.

8.6.227. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.

8.6.228. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.

8.6.229. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.

8.6.230. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.

8.6.231. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:

- Czysty,
- Podejrzany,
- Bardzo podejrzany,
- Szkodliwy.

8.6.232. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

8.6.233. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.

8.6.234. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

8.7. Szyfrowanie

8.7.235. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 32-bit i 64-bit i Windows 11-64bit.

8.7.236. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku macOS 10.14 lub nowszej.

8.7.237. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).

8.7.238. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.

8.7.239. Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.

8.7.240. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.

8.7.241. Aplikacja musi mieć możliwość korzystania z technologii TCG OPAL - dyski sprzętowo szyfrowane.

8.7.242. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

8.7.243. W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.

8.7.244. Aplikacja do szyfrowania musi być zarządzana z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej.

8.7.245. Konsola centralnego zarządzania musi pozwalać na wygenerowanie, dla każdej zaszyfrowanej stacji, dysku ratunkowego.

8.7.246. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:

- ilość znaków,
- czy hasło ma zawierać wielkie litery,
- czy hasło ma zawierać małe litery,
- czy hasło ma zawierać cyfry,
- czy hasło ma zawierać znaki specjalne,
- okres ważności,
- ilość nieudanych logowań,
- możliwość zmiany hasła.

8.7.247. Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom.

8.7.248. Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku.

8.8. Zarządzanie podatnościami i aktualizacjami

8.8.249. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.

8.8.250. Baza wykrywanych podatności musi zawierać minimum 35000 CVE.

8.8.251. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych komponentów na stacjach końcowych.

8.8.252. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.

8.8.253. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:

- nazwę aplikacji lub systemu operacyjnego,
- punktacje CVSS,
- opis wykrytej podatności,
- wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta.

8.8.254. Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach.

8.8.255. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.

8.8.256. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.

8.8.257. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.

8.8.258. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.

8.8.259. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.

8.8.260. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.

8.8.261. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.

8.8.262. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.

8.9. Extended detection & response Serwer

8.9.263. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych.

8.9.264. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
8.9.265. System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.
8.9.266. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
8.9.267. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
8.9.268. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
8.9.269. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
8.9.270. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
8.9.271. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica".
8.9.272. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
8.9.273. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8.9.274. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
8.9.275. Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne.
8.9.276. Serwer administracyjny musi oferować możliwość blokowania plików po sumachkontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
8.9.277. Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali.
8.9.278. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnychna stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
8.9.279. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
8.9.280. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
8.9.281. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.

8.9.282. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
8.9.283. Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy.
8.9.284. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
8.9.285. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal).
8.9.286. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8.9.287. Konsola administracyjna musi mieć możliwość tagowania obiektów.
8.9.288. Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli.
8.9.289. Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci.
8.9.290. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
8.9.291. Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.

8.10. Konektor

8.10.292. Pełne wsparcie dla systemu Windows 10/ Windows 11 oraz Windows Server 2012/2012R2/2016/2019/2022.
8.10.293. Pełne wsparcie dla systemów macOS 10.15 i nowszych.
8.10.294. Pełne wsparcie dla systemów Linux RHEL 7.6+/RHEL 8/RHEL 9/Ubuntu 18.04/Ubuntu 20.04/Ubuntu 22.04/Debian 10/Debian 11/Debian 12
8.10.295. Wsparcie dla 32 i 64-bitowej wersji systemu Windows.
8.10.296. Konektor musi współpracować z produktem antywirusowym tego samego producenta.
8.10.297. Konektor nie może działać bez produktu antywirusowego tego samego producenta.
8.10.298. W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonane przez konektor.
8.10.299. Połączenie konektora do serwera zarządzającego musi być szyfrowane.

8.10.300. Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane.

8.11. Ochrona poprzez dwuskładnikowe uwierzytelnianie

8.11.301. Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.

8.11.302. Rozwiązanie musi wspierać system operacyjne Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11.

8.11.303. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.

8.11.304. Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019.

8.11.305. Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016.

8.11.306. Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 /2019.

8.11.307. Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access.

8.11.308. Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Ac- cess.

8.11.309. Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access.

8.11.310. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnia - nie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.

8.11.311. Oprogramowanie musi integrować się z systemem Windows Server poprzez konsolę MMC (Microsoft Managment Console).

8.11.312. Moduł zarządzania uwierzytelnianiem się użytkowników musi integrować się z wbudowanym w systemie Windows Server modułem do zarządzania kontami użytkowników (ADUC) w postaci dodatkowej zakładki we właściwościach użytkownika.

8.11.313. Administrator musi mieć możliwość określenia z jakiej metody uwierzytelniania użytkownicy będą korzystać:

- dwuskładnikowe uwierzytelnianie poprzez użycie aplikacji mobilnej zainstalowanej na urządzeniu mobilnym użytkownika,
- dwuskładnikowe uwierzytelnianie poprzez wiadomości SMS wysyłane do użytkowników,
- klasyczna uwierzytelnianie (przy użyciu nazwy użytkownika i hasła).

8.11.314. Administrator musi mieć możliwość wysłania w postaci wiadomości SMS odnośnika, za pomocą którego użytkownik może pobrać i zainstalować dedykowaną aplikację mobilną wspierającą systemy mobilne opisane w punkcie 28 niniejszej specyfikacji.

8.11.315. Dwuskładnikowe uwierzytelnianie nie może wymagać od użytkownika instalacji aplikacji mobilnej w telefonie - wówczas jednorazowe hasła muszą być przesyłane do użytkownika w postaci wiadomości SMS.

8.11.316. Dodatek w module ADUC musi wyświetlać informację co najmniej o dniu i godzinie ostatniej próby logowania oraz ostatniej nieudanej próby logowania użytkownika.

8.11.317. Oprogramowanie musi posiadać mechanizm zabezpieczający przed atakiem typu brute-force, które po określonej liczbie prób nieudanego logowania musi automatycznie zablokować możliwość uwierzytelnienia się dla danego użytkownika.

8.11.318. Administrator musi mieć możliwość odblokowania konta użytkownika w celu umożliwienia ponownego dostępu.

8.11.319. Administrator musi mieć możliwość wymuszenia zabezpieczenia aplikacji mobilnej za pomocą kodu PIN lub za pomocą danych biometrycznych – wówczas każdy użytkownik instalujący aplikację mobilną bez nadania kodu PIN nie będzie mógł generować jednorazowych haseł (OTP).

8.11.320. Administrator musi mieć możliwość podglądu informacji na temat:

- aktualnego stanu licencji,
- ilości wykorzystanych licencji (użytkowników),
- ilości pozostałych do wykorzystania wiadomości SMS.

8.11.321. Oprogramowanie przy użyciu serwera RADUIS musi umożliwiać dostęp do zabezpieczonych zasobów za pomocą klasycznej metody uwierzytelnienia (nazwa użytkownika i hasła).

8.11.322. Administrator musi mieć możliwość wyboru, którzy użytkownicy będą korzystać z dwuskładnikowego uwierzytelniania.

8.11.323. Administrator musi mieć możliwość ograniczenia dostępu przy uwierzytelnianiu metodą RADIUS do grupy użytkowników wskazanych w konfiguracji.

8.11.324. Jednorazowe hasło (OTP) generowane przez użytkowników powinno być unikalne i może być użyte tylko raz – nie dopuszcza się wielokrotnego użycia tego samego OTP.

8.11.325. Do wysyłania wiadomości SMS nie może być wymagane posiadanie własnej bramy SMS i centrali GSM.

8.11.326. Wysyłanie wiadomości SMS z hasłami jednorazowymi musi odbywać się z infrastruktury producenta rozwiązania.

8.11.327. Wysyłanie wiadomości musi być możliwe w przypadku telefonów pracujących w roamingu.

8.12. API i SDK

8.12.328. Producent musi udostępnić API pozwalające programistom na zintegrowanie rozwiązania z serwisem web lub oprogramowaniem wykorzystującym uwierzytelnianie w oparciu o usługę Active Directory.

8.12.329. Producent musi udostępniać SDK w celu umożliwienia programistom implementacji dwuskładnikowego uwierzytelniania dla środowisk nie wykorzystujących usługi Active Directory do uwierzytelniania użytkowników (np. wykorzystujących własną bazę danych z użytkownikami).

8.12.330. SDK musi być dostarczone zarówno dla platformy Microsoft .NET jak i języków programowania PHP i Java.

8.13. Aplikacja mobilna

8.13.331. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).

8.13.332. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.

8.13.333. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.

8.13.334. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego użytkowników poprzez dwuskładnikowe uwierzytelnianie.

8.13.335. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

9. Opis równoważności.

9.1. Zamawiający dopuszcza możliwość dostawy rozwiązania równoważnego do opisanych w pkt. 8.

9.2. Za rozwiązanie równoważne Zamawiający uzna rozwiązanie spełniające wymagania opisane w pkt. 8 oraz poniższe wymagania:

9.2.1. Dostawę oprogramowania o funkcjonalności nie gorszej od posiadanych przez Zamawiającego.

9.2.2. Zapewnienie usługi kompletnej nieinwazyjnej deinstalacji dotychczasowego oprogramowania antywirusowego i oprogramowania antyspamowego z całej infrastruktury informatycznej (komputerów, serwerów i urządzeń mobilnych) Zamawiającego.

9.2.3. Zapewnienie usługi kompletnej nieinwazyjnej instalacji i konfiguracji nowego rozwiązania w infrastrukturze informatycznej Zamawiającego.

9.2.4. Zapewnienia dodatkowego wsparcia technicznego (zdalnego oraz, w razie potrzeby, bezpośredniego – realizowanego w siedzibie Zamawiającego) przez Wykonawcę przez okres miesiąca od daty wdrożenia produkcyjnego rozwiązania równoważnego.

9.2.5. Przeszkolenie pracownika Zamawiającego z zakresu obsługi, konfiguracji i administracji całości rozwiązania równoważnego.

9.2.6. Wdrożenie, szkolenie, asysta techniczna i dodatkowe wsparcie techniczne Wykonawcy – w języku polskim w siedzibie Zamawiającego.

9.2.7. Usługi wdrożeniowe równoważnego oprogramowania antywirusowego i oprogramowania antyspamowego zostaną zrealizowane przez Wykonawcę nie później niż w terminie wygaśnięcia posiadanych przez Zamawiającego licencji.

9.3. Oprogramowanie nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie z art. 4 pkt. 7 Ustawy o Krajowym systemie cyberbezpieczeństwa (tj. Dz. U z 2018r. poz. 1560), dalej:

„Ustawa”, należy do Krajowego systemu cyberbezpieczeństwa, którego celem jest zgodnie z art. 3 Ustawy, zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Tym samym, Oprogramowanie musi być zgodne z celem Krajowego

systemu cyberbezpieczeństwa i przepisami Ustawy oraz nie zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa.

9.4. Warunki licencjonowania mają umożliwiać Zamawiającemu (Licencjobiorcy) objęcie dostarczonym oprogramowaniem stacji roboczych należących do podmiotów administracji publicznej, na warunkach zdefiniowanych w dokumencie OPZ.

9.5. Dostarczana licencja Oprogramowania musi pochodzić z autoryzowanego przez producenta kanału dystrybucji. Wykonawca jest zobowiązany dostarczyć Zamawiającemu dowody poświadczające autentyczność zakupionych licencji na zasadach określonych przez producenta wraz z dostawą Oprogramowania.