ZP.271.01.08.2026

Załącznik nr 3

OPIS PRZEDMIOTU ZAMÓWIENIA

zakup i dostawa urządzeń oraz oprogramowania w ramach realizacji projektu pn.: "Cyberbezpieczny samorząd", współfinansowany z Funduszy Europejskich na Rozwój Cyfrowy (FERC) za pośrednictwem Europejskiego Funduszu Rozwoju Regionalnego (EFRR) w ramach Priorytetu II Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa., nr umowy FERC.02.02-CS.01-001/23/0872

Nr/znak nadany sprawie przez Zamawiającego: ZP.271.01.08.2026

1.Oprogramowanie;

Lp.	Nazwa	Wymagane parametry techniczne	ilość
1.	Ochrona Endpoint	Ochrona stacji roboczych - Windows 1. Rozwiązanie musi wspierać systemy Windows 10/Windows 11. 2. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows. 3. Rozwiązanie musi wspierać architekturę ARM64. 4. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. 5. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. 6. Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim. 7. Skuteczność rozwiązania potwierdzona nagrodami VB100 i AV-comparatives. Ochrona antywirusowa i antyspyware 8. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 9. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 10. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami. 11. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 12. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje. 13. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. 14. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu. 15. 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. 16. 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). 17. Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 18. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 19. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych. 20. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. 21. Rozwiązanie musi posiadać możliwość ubezter zczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 22. Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku. 23. Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 24. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. 25. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera. 26. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. 27. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 28. 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. 29. Rozwiązanie musi posiadać wbudowany konektor dla programu Microsoft Outlook. 30. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu Microsoft Outlook. 31. 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). 32. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 33. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 34. Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie. 35. 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. 36. Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora. 37. Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 38. Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 39. Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe. 40. Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta. 41. Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego. 42. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 43. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym. 44. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 45. 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. 46. 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. 47. 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. 48. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 49. Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika. 50. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 51. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. 52. 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. 53. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo. 54. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji. 55. 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. 56. 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. 57. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. 58. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. 59. 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. 60. 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. 61. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. 62. 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. 63. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 64. W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 65. Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika. 66. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS). 67. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, d. 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, e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 68. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.	

		69. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. 70. Rozwiązanie musi posiadać zaawansowany skaner pamięci. 71. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych. 72. 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. 73. 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. 74. 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. 75. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 76. 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. 77. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji. 78. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. 79. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. 80. Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). 81. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 82. Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym. 83. W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania.	

		84. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym. 85. Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń. 86. Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji. 87. 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. 88. Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie. 89. 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. 90. W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji. 91. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej. 92. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia. 93. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny. 94. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. 95. Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki. 96. 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. 97. Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji. 98. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie. 99. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 100. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.	

		101. Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup. 102. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny. 103. Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść” 104. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. 105. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. 106. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. 107. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 108. Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet. 109. Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB. 110. Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. 111. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu. Ochrona przed spamem 112. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 113. Rozwiązanie musi umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. 114. Rozwiązanie musi umożliwiać automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. 115. Rozwiązanie musi posiadać możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego. 116. Rozwiązanie musi posiadać możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego. 117. Rozwiązanie musi posiadać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam. 118. Rozwiązanie musi możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.	

		119. Rozwiązanie musi domyślnie współpracować z folderem „Wiadomości-śmieci”, dostępnym w programie Microsoft Outlook. 120. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana” 121. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana”. 122. Rozwiązanie musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera. Zapora osobista (personal firewall) 123. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: a. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, b. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, c. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, d. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. 124. Rozwiązanie musi oceniać reguły zapory systemu Windows. 125. Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych. 126. Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie. 127. 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. 128. Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj. 129. Rozwiązanie musi posiadać możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji. 130. 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. 131. Rozwiązanie musi wykrywać modyfikację w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu. 132. Rozwiązanie musi posiadać możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.	

		133. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci. 134. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. 135. 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. 136. 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. 137. 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. 138. Rozwiązanie musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów: a. z aplikacją lokalną, którą administrator wskazuje z listy, b. z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP. Kontrola dostępu do stron internetowych 139. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 140. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory. 141. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 142. 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. 143. Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych. 144. Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta. 145. Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.	

		146. Rozwiązanie musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj. 147. Rozwiązanie musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej. Bezpieczna przeglądarka 148. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. 149. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 150. Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki. 151. Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę. 152. Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki. 153. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.	
2.	Ochrona Endpoint dla Android	Ochrona urządzeń mobilnych opartych o system Android 1. Rozwiązanie musi wspierać system co najmniej Android 6.0. 2. Rozwiązanie musi wspierać rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa. 3. Rozwiązanie musi wspierać procesory: ARM z obsługą ARMv7 lub x86 Intel Atom. 4. Rozwiązanie musi posiadać ochronę plików w czasie rzeczywistym. 5. Rozwiązanie musi posiadać ochronę przed atakami typu „phishing”. 6. Rozwiązanie musi skanować wszystkie typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 7. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 8. Rozwiązanie musi posiadać ochronę proaktywną wykrywającą nieznane zagrożenia. 9. W przypadku wykrycia zagrożenia użytkownik musi otrzymać odpowiednie powiadomienie. 10. Rozwiązanie musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia. 11. Rozwiązanie musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). Skanowanie na żądanie: 12. Rozwiązanie musi mieć możliwość skanowania zainstalowanych aplikacji. 13. Informacje o skanowaniu mają być przechowywane w plikach dziennika.	

		14. Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania. 15. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia. Polityka ustawień: 16. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej: a. połączenie Wi-Fi, b. GPS, c. usługi lokalizacyjne, d. pamięć, e. roaming danych, f. roaming połączeń, g. nieznane źródła, h. tryb debugowania, i. komunikacja NFC, j. szyfrowanie pamięci masowej, k. urządzenie zrootowane. Kontrola aplikacji: 17. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji. 18. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji. 19. Blokowanie aplikacji musi być możliwe w oparciu o: a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła. Zabezpieczenia urządzenia: 20. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej: a. minimalny poziom zabezpieczeń i złożoność blokady ekranu, b. maksymalną dopuszczaną liczbę błędnych prób odblokowania, c. odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie, d. czas, po którym automatycznie nastąpi blokada ekranu, e. ograniczenie dostępu do kamery wbudowanej w urządzenie. Aktualizacje modułów: 21. Rozwiązanie musi umożliwiać wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji. 22. Rozwiązanie musi mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą	

		aktualizacje modułów co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin. 23. Rozwiązanie musi posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją. Konfiguracja i zdalne zarządzanie: 24. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne. 25. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.	
3.	Ochrona usług chmurowych	Ochrona usługi Microsoft 365 1. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams. 2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365. 3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną. 4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci. 5. Rozwiązanie musi być dostępny w języku polskim. 6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej: a. użytkowników, otrzymujących najwięcej spamu, b. użytkowników, otrzymujących najwięcej wiadomości typu „phishing”, c. użytkowników, otrzymujących największą ilość szkodliwego oprogramowania, d. kont użytkowników, które mogę być podejrzane. 7. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive. 8. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej: a. jaka ilość wiadomości została przeskanowania, b. wynik skanowania poszczególnej wiadomości, c. czynność podjęta przez rozwiązanie. 9. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o: a. zagrożeniach, które zostały wykryte, b. na jakim koncie zostały wykryte, c. jakie zagrożenie zostało wykryte, d. podjętą czynność. 10. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive. 11. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem. 12. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.	

		13. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej: a. wykorzystania do analizy mechanizmów chmurowych, tego samego producenta, b. wprowadzenia białych i czarnych list adresów ochrony Exchange'a Online, c. dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing. 14. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day. 15. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta. 16. Funkcja ochrony przed zagrożeniami 0-day 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. 17. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 18. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.	
4.	Rozszerzone wykrywanie	Serwer 1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych. 2. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. 3. System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta. 4. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych. 6. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 7. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 8. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 9. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica". 10. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 11. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 12. 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. 13. Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne. 14. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 15. Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali. 16. 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. 17. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 18. 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. 19. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 20. 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. 21. Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy. 22. 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.	

		23. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal). 24. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 25. Konsola administracyjna musi mieć możliwość tagowania obiektów. 26. Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli. 27. Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci. 28. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell. 29. Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł. Konektor 1. Pełne wsparcie dla systemu Windows 10/ Windows 11 oraz Windows Server 2012/2012R2/2016/2019/2022. 2. Pełne wsparcie dla systemów macOS 10.15 i nowszych. 3. 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 4. Wsparcie dla 32 i 64-bitowej wersji systemu Windows. 5. Konektor musi współpracować z produktem antywirusowym tego samego producenta. 6. Konektor nie może działać bez produktu antywirusowego tego samego producenta. 7. W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonane przez konektor. 8. Połączenie konektora do serwera zarządzającego musi być szyfrowane. 9. Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane.	
5.	Szyfrowanie	1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 32-bit i 64-bit i Windows 11-64bit. 2. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku macOS 10.14 lub nowszej. 3. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 4. 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. 5. Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim. 6. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.	

		7. Aplikacja musi mieć możliwość korzystania z technologii TCG OPAL - dyski sprzętowo szyfrowane. 8. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. 9. 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. 10. Aplikacja do szyfrowania musi być zarządzana z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej. 11. Konsola centralnego zarządzania musi pozwalać na wygenerowanie, dla każdej zaszyfrowanej stacji, dysku ratunkowego. 12. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej: a) ilość znaków, b) czy hasło ma zawierać wielkie litery, c) czy hasło ma zawierać małe litery, d) czy hasło ma zawierać cyfry, e) czy hasło ma zawierać znaki specjalne, f) okres ważności, g) ilość nieudanych logowań, h) możliwość zmiany hasła. 13. Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom. 14. Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku.	
6.	Ochrona serwera pocztowego MS Exchange	1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych. 2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019. 3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub. 4. Rozwiązanie musi umożliwiać Administratorowi na etapie instalacji wybór komponentów jakie mają być zainstalowane. 5. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange. 6. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI. 7. Rozwiązanie musi mieć możliwość zdefiniowania ilości wątków skanujących w celu optymalizacji pracy serwera. Liczba wątków skanowania musi wynosić od 1 do 21. 8. Rozwiązanie musi zapewnić skanowanie przed zapisaniem wiadomości w bazie danych przy pomocy transport agenta. 9. W przypadku wykrycia wirusa/blokowania wiadomości rozwiązanie musi umożliwić usunięcie wiadomości/ załącznika, podmianę załącznika na czysty plik zawierający jedynie informację o infekcji. 10. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po	

		zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum. 11. Rozwiązanie musi posiadać możliwość tworzenia białych i czarnych list domen/adresów IP, adresów e-mail. 12. Rozwiązanie musi posiadać możliwość akceptacji białych list stworzonych na poziomie serwera MS Exchange. 13. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty. 14. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty. 15. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja. 16. Program ma posiadać mechanizm greylisting (szara lista). 17. Rozwiązanie musi posiadać możliwość tworzenia wyjątków dla mechanizmu szarej listy. 18. Rozwiązanie musi posiadać możliwość stworzenia kwarantanny poczty per użytkownik. 19. Kwarantanna musi być dostępna dla użytkownika końcowego za pośrednictwem przeglądarki WWW. 20. Pliki zapisywane w katalogu kwarantanny muszą być szyfrowane. 21. Użytkownik końcowy musi posiadać możliwość zarządzania wiadomościami znajdującymi się w kwarantannie w tym co najmniej, mieć możliwość uwolnienia wiadomości z kwarantanny, jej usunięcia lub pozostawienia w kwarantannie. 22. Administrator musi mieć możliwość wglądu w globalną kwarantannę z poziomu interfejsu aplikacji oraz przeglądarki WWW. 23. Rozwiązanie musi umożliwiać przesyłanie raportów dotyczących plików poddanych kwarantannie na wskazany adres e-mail. 24. Rozwiązanie musi umożliwiać pominięcie reguł kwarantanny podczas zwolnienia wiadomości e-mail w środowisku klastrowym. 25. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików serwera „na żądanie” lub według harmonogramu. 26. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 27. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami. 28. Rozwiązanie musi posiadać wbudowaną technologię ochrony przed atakami typu backscatter.	

		29. Rozwiązanie musi umożliwiać zaawansowane skanowanie przy użyciu interfejsu AMSI. 30. Rozwiązanie musi posiadać wbudowany skaner UEFI. 31. Rozwiązanie musi umożliwiać skonfigurowanie wyjątków ochrony przed atakami sieciowymi (IDS). 32. Rozwiązanie musi umożliwiać wykrywanie włamań wykorzystujących protokoły: SMB, RPC, RDP i informować użytkownika o wykryciu ataku. 33. Rozwiązanie musi wyświetlać powiadomienia po wykryciu ataku. 34. Rozwiązanie musi zezwalać na połączenia przychodzące do udziałów administracyjnych po protokole SMB. 35. Rozwiązanie musi odmawiać połączenia starym (nieobsługiwanym) dialektom protokołu SMB oraz zabezpieczeniom tego protokołu bez rozszerzeń zabezpieczeń. 36. Rozwiązanie musi umożliwiać komunikację z usługą menadżera konta zabezpieczeń, urząd zabezpieczeń lokalnych, rejestr zdalny, service control manager, usługą serwera i innymi usługami. 37. Rozwiązanie musi posiadać wbudowany skaner skryptów JavaScript, wykonywanych przez przeglądarki internetowe. 38. Rozwiązanie musi umożliwiać zdefiniowanie listy aplikacji, dla których jest przeprowadzane filtrowanie protokołu SSL/TLS. 39. Rozwiązanie musi umożliwiać określenie białej listy domen, dla których analiza protokoły SSL/TLS nie będzie wykonywana. 40. Rozwiązanie musi umożliwiać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 41. Rozwiązanie musi umożliwiać skanowanie plików spakowanych i skompresowanych. 42. Rozwiązanie musi posiadać wbudowaną technologię monitorowania zdarzeń bezpieczeństwa związanych z zagrożeniami typu malware, exploit, PUA, podłączenia do sieci Botnet. 43. Musi być możliwe uruchamianie modułu ochrony przed złośliwym oprogramowaniem w ramach usługi chronionej systemu Windows (dla systemów Windows Server 2012 R2 lub nowszych). 44. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 45. Rozwiązanie musi wykorzystywać technologię chmury w celu przyśpieszenia reakcji na nowe zagrożenia oraz optymalizacji samego procesu skanowania. 46. Rozwiązanie musi umożliwiać analizę zagrożeń przez porównanie skanowanych plików z białą i czarną listą obiektów w chmurze producenta. 47. Rozwiązanie musi umożliwiać wybór jakie typy podejrzanych próbek będą przesyłane do producenta. W	

		tym co najmniej: pliki wykonywalne, archiwa, skrypty, możliwy SPAM. 48. Rozwiązanie musi umożliwiać określenie plików i folderów, które nigdy nie będą przesyłane do producenta w celu analizy, np. plików zawierających informacje poufne. 49. Rozwiązanie musi umożliwiać zapisywanie informacji diagnostycznych w dziennikach dla aparatu antyspamowego. 50. Rozwiązanie musi być wyposażone w mechanizm chroniący serwer przed exploitami i atakami typu 0-day. 51. Rozwiązanie musi posiadać zaawansowany skaner pamięci umożliwiający wykrywanie zagrożeń próbujących działać na poziomie pamięci operacyjnej serwera. 52. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS). 53. Rozwiązanie musi w natywny sposób wspierać środowiska klastrowe. 54. Rozwiązanie musi umożliwiać wskazanie zewnętrznych lokalizacji w których przechowywane będą moduły i aktualizacje programu. 55. Rozwiązanie musi wspierać WMI za pomocą których może przekazywać podstawowe informacje na temat swojej pracy do zewnętrznych systemów np. SIEM. 56. Rozwiązanie musi skanować i oczyszczać w czasie rzeczywistym pocztę przychodzącą i wychodzącą, która jest obsługiwana przy pomocy programu Microsoft Outlook zainstalowanego lokalnie na serwerze pocztowym. 57. Rozwiązanie musi posiadać wbudowaną ochronę przed atakami typu phishing w wiadomościach e-mail. 58. Rozwiązanie musi umożliwiać skanowanie w środowiskach hybrydowych opartych na MS Office 365. 59. Rozwiązanie musi umożliwiać ochronę dostępu do urządzeń według zdefiniowanych reguł w określonych przedziałach czasu. 60. Rozwiązanie musi tworzyć log ochrony protokołu SMTP. 61. Rozwiązanie musi mieć możliwość utworzenia kilku zadań skanowania (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (metody skanowania, obiekty skanowania, czynności). 62. Rozwiązanie musi umożliwiać aktualizację modułów ochrony bez konieczności re instalacji całego programu. 63. Rozwiązanie musi uruchamiać jeden skaner uruchamiany w pamięci, do którego odnoszą się wszystkie monitory skanujące i skanery na żądanie. 64.Rozwiązanie musi mieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach oraz procesów. 65. Administrator ma możliwość dodania wykluczenia ze skanowania po tzw. HASH'u, wskazującym bezpośrednio na określoną infekcję, a nie konkretny plik.	

		66. Rozwiązanie musi być wyposażone w dwa niezależnie pracujące mechanizmy analizy heurystycznej (standardowa i zaawansowana heurystyka). 67. Administrator musi posiadać możliwość używania jednego poziomu analizy heurystycznej lub obu poziomów jednocześnie. 68. Rozwiązanie musi umożliwiać automatyczne wysyłanie nowych zagrożeń (wykrytych przez heurystykę) do laboratorium producenta przez program antywirusowy – nie wymaga ingerencji użytkownika. 69. Wysyłanie nowych zagrożeń musi być możliwe za pomocą interfejsu rozwiązania i nie może do tego celu wykorzystywać klienta pocztowego zainstalowanego w systemie. 70. Rozwiązanie musi umożliwiać wysyłanie wraz z próbką adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 71. W przypadku wykrycia wirusa, ostrzeżenie może zostać wysłane do administratora poprzez e-mail. 72. Rozwiązanie musi posiadać wbudowany dziennik zdarzeń rejestrujący informacje na temat znalezionych wirusów, dokonanych aktualizacji baz wirusów i wersji oprogramowania. 73. Administrator musi mieć możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu. 74. Możliwość zabezpieczenia hasłem musi obejmować wyłączenie rozwiązaniaantywirusowego oraz jego odinstalowanie. 75. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 76. Rozwiązanie musi być dostępne z Internetu, lokalnego zasobu sieciowego, nośnika CD/DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP). 77. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. 78. Rozwiązanie musi wspierać aktualizacje za pośrednictwem serwera Proxy. 79. Administrator musi posiadać możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami. 80. Rozwiązanie musi rejestrować wszystkie dane transmitowane za pośrednictwem funkcji ochrony sieci w formacie PCAP. 81. Rozwiązanie musi umożliwiać zarejestrowanie dodatkowych informacji na temat systemu operacyjnego, na przykład dotyczące uruchomionych procesów, aktywności procesora o działania dysku. 82. Rozwiązanie musi rejestrować komunikację produktu z serwerami licencji producenta.	

		83. Rozwiązanie musi automatycznie przesyłać powiadomienia o zdarzeniach pocztą e-mail na wskazany adres e-mailowy. 84. Musi istnieć możliwość zdefiniowania wykorzystywanego zestawu znaków. W tym co najmniej: Unicode (UTF-8), Ascii (7-bit), Japanese (ISO-2022-JP), lokalne. 85. Rozwiązanie musi posiadać wsparcie dla RMM (Remote Monitoring and Management). 86. Rozwiązanie musi posiadać możliwość zdalnej administracji za pomocą konsoli administracji zdalnej. 87. Rozwiązanie musi posiadać wbudowany, dedykowany moduł command line umożliwiający konfigurację oraz uruchamianie zadań zainstalowanej aplikacji. 88. Rozwiązanie musi być wyposażone w narzędzie umożliwiające wygenerowanie raportu dotyczącego stanu komputera, w tym co najmniej zainstalowanych aplikacji, uruchomionych procesów, ważnych wpisów w rejestrze i uruchomionych usług. 89. Do administracji zdalnej musi być wykorzystywany dedykowany agent. 90. Agent musi komunikować się z serwerem administracji zdalnej w bezpieczny sposób uniemożliwiający podsłuch komunikacji. 91. Skuteczność programu ma być potwierdzona nagrodami niezależnych organizacji (np. VB100, ISCA labs, Check Mark). 92. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.	
7.	Ochrona poprzez dwuskładnikowe uwierzytelnianie	1. 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. 2. Rozwiązanie musi wspierać system operacyjne Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11. 3. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows. 4. Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019. 5. Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016. 6. Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 /2019. 7. Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access. 8. Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Ac-cess. 9. Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access. 10. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnia-nie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.	

		11. Oprogramowanie musi integrować się z systemem Windows Server poprzez konsolę MMC (Microsoft Managment Console). 12. 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. 13. 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) 14. 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. 15. Dwuskładnikowe uwierzytelnianie nie może wymagać od użytkownika instalacji aplikacji mobilnej w telefonie - wówczas jednorazowe hasła muszą być przesyłane do użytkownika w postaci wiadomości SMS. 16. Dodatek w module ADUC musi wyświetlać informację co najmniej o dniu i godzinie ostatniej próby logowania oraz ostatniej nieudanej próby logowania użytkownika. 17. 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. 18. Administrator musi mieć możliwość odblokowania konta użytkownika w celu umożliwienia ponownego dostępu. 19. 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). 20. Administrator musi mieć możliwość podglądu informacji na temat: - aktualnego stanu licencji - ilości wykorzystanych licencji (użytkowników) - ilości pozostałych do wykorzystania wiadomości SMS. 21. Oprogramowanie przy użyciu serwera RADUIS musi umożliwiać dostęp do zabezpieczonych zasobów za pomocą klasycznej metody uwierzytelnienia (nazwa użytkownika i hasła). 22. Administrator musi mieć możliwość wyboru, którzy użytkownicy będą korzystać z dwuskładnikowego uwierzytelniania.	

		23. Administrator musi mieć możliwość ograniczenia dostępu przy uwierzytelnianiu metodą RADIUS do grupy użytkowników wskazanych w konfiguracji. 24. Jednorazowe hasło (OTP) generowane przez użytkowników powinno być unikalne i może być użyte tylko raz – nie dopuszcza się wielokrotnego użycia tego samego OTP. 25. Do wysyłania wiadomości SMS nie może być wymagane posiadanie własnej bramy SMS i centrali GSM. 26. Wysyłanie wiadomości SMS z hasłami jednorazowymi musi odbywać się z infrastruktury producenta rozwiązania. 27. Wysyłanie wiadomości musi być możliwe w przypadku telefonów pracujących w roamingu. API i SDK 28. Producent musi udostępnić API pozwalające programistom na zintegrowanie rozwiązania z serwisem web lub oprogramowaniem wykorzystującym uwierzytelnianie w oparciu o usługę Active Directory. 29. 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). 30. SDK musi być dostarczone zarówno dla platformy Microsoft .NET jak i języków programowania PHP i Java. Aplikacja mobilna 31. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej). 32. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN. 33. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline. 34. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego użytkowników poprzez dwuskładnikowe uwierzytelnianie. 35. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.	
8.	Ochrona serwera Windows	1. Rozwiązanie musi posiadać wsparcie dla systemów Microsoft Windows Server 2012 i nowszych. 2. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. 3. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 4. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.	

		6. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje. 7. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. 8. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu. 9. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). 10. Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 11. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 12. Rozwiązanie ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 13. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych. 14. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. 15. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 16. Rozwiązanie musi wspierać mechanizm klastrowania. 17. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS). 18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, d. 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, e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 19. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe,	

		aplikacje docelowe, elementy docelowe rejestru systemowego. 20. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. 21. Rozwiązanie musi posiadać zaawansowany skaner pamięci. 22. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych. 23. Rozwiązanie musi oferować możliwość skanowania dysków sieciowych typu NAS. 24. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze. 25. Rozwiązanie musi 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. 26. Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 27. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. 28. 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. 29. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 30. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. 31. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 32. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 33. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. 34. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.	

		35. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. 36. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 37. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. 38. Rozwiązanie ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 39. 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. 40. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne –jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sz tucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 41. 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. 42. Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 43. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 44. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 45. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail. 46. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. 47. Rozwiązanie musi posiadać możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło. 48. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo. 49. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym	

		użytkownika i wyświetlić listę niezainstalowanych aktualizacji. 50. 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. 51. 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. 52. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. 53. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. 54. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, 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. 55. 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. 56. Rozwiązanie musi oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. 57. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 58. 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. 59. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji. 60. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. 61. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. 62. Rozwiązanie musi być wyposażone w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). 63. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają	

		wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 64. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 65. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 66. Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania. 67. Rozwiązanie musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”. 68. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 69. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia. 70. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 71. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 72. Rozwiązanie musi posiadać ochronę przed przyłączeniem komputera do sieci botnet. 73. Rozwiązanie musi mieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 74. Rozwiązanie musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów. 75. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. 76. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. 77. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 78. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu	
9.	Zarządzanie podatnościami i aktualizacjami	1. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.	

		2. Baza wykrywanych podatności musi zawierać minimum 35000 CVE. 3. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych komponentów na stacjach końcowych. 4. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie. 5. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum: a. nazwę aplikacji lub systemu operacyjnego b. punktacje CVSS c. opis wykrytej podatności d. wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta 6. Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach. 7. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji. 8. 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. 9. 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. 10. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach. 11. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze. 12. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania. 13. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania. 14. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności. Ilość obsługiwanych stanowisk Min. 26 Licencja 24 miesięczna Instalacja i konfiguracja systemu na serwerze i na 26 stanowiskach roboczych	

10.	Funkcje realizowane przez oprogramowanie	• Możliwość backupu X komputerów, Y serwerów, Z hostów wirtualizacji (np.: 100 stacji, 10 serwerów, 2 hosty) • Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich • Program serwerowy kompatybilny z systemami: Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology • Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, Linux, BSD, Mac OS X, QNAP, Synology • Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików) • **Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)** • Automatyczny **backup przy wyłączaniu komputera** • Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i ? • Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows) • Backup baz danych i plików poczty w trybie online i offline • Kopie rotacyjne (wersjonowanie) • **Zapis archiwów w otwartym formacie (ZIP 64-bit)** • Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi • Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore) • Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej • Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych • Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO • Kompresja po stronie stacji roboczej • Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP, • Replikacja na napęd optyczny: CD, DVD, Blu-Ray, HD-DVD i napęd taśmowy: DDS, DLT, LTO, AIT (tylko Windows) • Centralne sterowanie całym Systemem z jednego miejsca • Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników	

		• Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN • Wysyłanie Alertów administracyjnych na e-mail • Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych • Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki • Automatyczna aktualizacja oprogramowania na komputerach zdalnych • Bezterminowa licencja - licencja nie może być ograniczona czasowo • Interfejs, instrukcja i pomoc techniczna w języku polskim • Obsługa min. 30 komputerów i 2 serwerów • Instalacja i konfiguracja na maksymalnie 30 komputerach i na serwerze	

2.Serwer z oprogramowaniem wraz z zasilaniem;

Lp.	Nazwa	Wymagane parametry techniczne	ilość
1.	Serwer z oprogramowaniem	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 4 dysków 3.5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 4 slotów przeznaczonych do instalacji pamięci DDR5 • Płyta główna powinna obsługiwać min. 128 pamięci RAM DDR5 • Dedykowany przez producenta procesora do pracy w serwerach • Taktowanie min. 2,6 GHz • Min. 8 rdzenie / 16 wątków • Minimum 64GB DDR5 UDIMM ECC 5600MT/s, • minimum jeden slot PCIe x8 • minimum jeden slot PCIe x16 • Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT • Dyski twarde: Zainstalowane 2 dyski SSD 2,5“ min 480 GB SATA Min. 2 dyski 4TB SAS 6Gbit/s 7,2tys. obr./min 3,5” dysk twardy Hot-Plug. • Kontroler RAID: Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10 • Min. 3 x USB z czego nie mniej niż 1x USB 3.2 pierwszej generacji	1 szt.

		• Min. 1x VGA • Min. 2 szt Redundantne, Hot-Plug min. 700W • System operacyjny/dodatkowe oprogramowanie: Windows Server 2025 Essentials • Bezpieczeństwo: Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). • Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela • Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie	

		dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: o Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. o Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. o Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia	

		wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. • Instalacja serwera w szafie RACK • Instalacja oprogramowania Windows	

3. Agregat prądotwórczy;

Lp.	Nazwa	Wymagane parametry techniczne	ilość
1.	Agregat prądotwórczy	Moc maksymalna Min. 16,00 kW Moc znamionowa Min. 14,00 kW Pojemność silnika Min. 800 cm3 Chłodzenie Powietrze Paliwo Benzyna Pojemność silnika Min. 890 cm3 Spalanie Max. 6,8 l / h przy obciążeniu 75 % Stabilizacja napięcia +- 2% Stopień ochrony prądnicy IP23 Rozruch Rozrusznik Zbiornik na paliwo Min. 42 l Waga Maks. 170 kg Wyposażenie • AVR • Gniazdo 230 V 16 A • Gniazdo 230 V 63 A • Zabezpieczenie przeciążeniowe • Czujnik ciśnienia oleju • Tłumik z przyłączem węża do spalin • Akumulator • Licznik czasu pracy	1 szt

		• Wąż do spalin	

UWAGA: W przypadku, gdy Zamawiający posługuje się w opisie przedmiotu zamówienia nazwami produktów dopuszcza się użycie przedmiotu równoważnego, który spełni minimalne standardy jakościowe, parametry techniczne, warunki docelowego przeznaczenia oraz funkcji i walorów użytkowych produktu wskazanego z nazwy. Nazwy handlowe produktów użyte w opisie przedmiotu zamówienia powinny być traktowanie jedynie jako definicje standardu jakiego wymaga Zamawiający.
Wykonawca określi cenę zakupu, dostawy w formularzu cenowym – załącznik nr 1 do zapytania ofertowego. Cena oferty musi uwzględniać wszystkie koszty niezbędne do realizacji zamówienia.
Cena może być tylko jedna za oferowany przedmiot zamówienia.
Oferowany sprzęt ma być fabrycznie nowy, nieużywany oraz nieeksponowany na wystawach lub imprezach targowych, sprawny technicznie, bezpieczny, kompletny i gotowy do pracy, a także musi spełniać wymagania techniczno-funkcjonalne wyszczególnione w opisie przedmiotu zamówienia.

Dorota Dąbrowska