Antyvirus

LICENCJA	W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje **czasową do dnia: 23/02/2026 r.** **Ilośc licencji: 55 szt.** Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie gwarancji. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta. Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.
Ochrona punktów końcowych urządzeń komputerowych	Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową. Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta. Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne: • Microsoft Windows 10 • Microsoft Windows 11 • macOS version 14 "Sonoma" • macOS version 13 "Ventura" • macOS version 12 "Monterey" Rozwiązanie dla ochrony antywirusowej systemów serwerowych wspiera następujące systemy operacyjne: • Microsoft® Windows Server 2016 Standard • Microsoft® Windows Server 2016 Essentials • Microsoft® Windows Server 2016 Datacenter • Microsoft® Windows Server 2016 Core • Microsoft® Windows Server 2019 Standard • Microsoft® Windows Server 2019 Essentials • Microsoft® Windows Server 2019 Datacenter • Microsoft® Windows Server 2019 Core • Microsoft® Windows Server 2022 Standard • Microsoft® Windows Server 2022 Essentials • Microsoft® Windows Server 2022 Datacenter • Microsoft® Windows Server 2022 Core Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej: • Microsoft Edge • Mozilla Firefox • Google Chrome • Safari

	Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika. Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej. Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej Opis technologii 1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity. 2. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransonmware. 3. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI) 4. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach. 5. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny. 6. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania. 7. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami. 8. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe. 9. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików. 10. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów. 11. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem. 12. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http. 13. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania. 14. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione. 15. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.

	16. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego. 17. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta. 18. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania. 19. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca. 20. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta. 21. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera. 22. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych. 23. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie. 24. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp. 25. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego. 26. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie. 27. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym 28. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji). 29. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów. 30. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów. 31. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit". 32. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne. 33. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na

	metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta. 34. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku. 35. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta. 36. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie. 37. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX. 38. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania. 39. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona. 40. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach. 41. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej. 42. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http. 43. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta. 44. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych. 45. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki. 46. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn. 47. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta. 48. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW. 49. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej. 50. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS. 51. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna".

	52. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów. 53. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp. 54. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn. 55. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego. 56. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup. 57. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej. 58. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji. 59. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej). 60. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora. 61. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych. 62. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV. 63. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji. 64. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji. 65. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie. 66. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów. 67. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć. 68. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.

	69. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji. 70. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces. 71. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej. 72. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego. 73. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej. 74. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej. 75. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth. 76. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej. 77. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy. 78. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu. 79. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach. 80. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego. 81. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu. 82. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware. 83. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS) 84. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji. 85. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji. 86. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików. 87. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania. **Centralna administracja** 1. Portal zarządzający jest dostępny w języku polskim.

	2. Poza językiem polskim konsola wspiera języki: angielski, niemiecki, francuski, hiszpański, fiński, włoski. 3. Logowanie do konsoli umożliwia wykorzystanie mechanizmów wieloskładnikowego uwierzytelniania (2FA) dla kont posiadających dostęp do konsoli zarządzającej. 4. Mechanizm 2FA służący zabezpieczeniu dostępu do konsoli zarządzającej w swoim działaniu wykorzystuje mechanizmy: powiadomień SMS, oraz tokenów jednorazowych generowanych w aplikacjach mobilnych (np. Google Authenticator, Microsoft Authenticator). 5. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej. 6. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta. 7. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. 8. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów. 9. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu. 10. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa. 11. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV. 12. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami. 13. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego. 14. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni. 15. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego. 16. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności. 17. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki. 18. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana. 19. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.

	20. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji. 21. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email. 22. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych. 23. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji. 24. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365. 25. Dodanie klucza licencyjnego skutkuje aktywacją zawartości dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym. 26. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego. 27. Profile mogą być przypisane do pojedynczych hostów lub do grup. 28. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD. 29. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny. 30. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi. 31. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji. 32. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach. 33. Pliki instalacyjne mają posiadać plików .EXE, .MSI .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent. 34. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika. 35. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów. 36. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego. 37. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji. 38. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.

	39. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.
Certyfikaty i standardy	• Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Products In Endpoint Protection Platforms Market na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/endpoint-protection-platforms minimalne wymaganie: minimalna liczba referencji 65 minimalna ocena z referencji 4,6 (załączyć wydruk) • Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Endpoint Detection and Response (EDR) Solutions Market https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions minimalne wymaganie: minimalna liczba referencji 17 minimalna ocena z referencji 4,4 (załączyć wydruk) system musi posiadać certyfikaty: • OPSWAT (dla EDR na poziomie min. Platinium), • AVLAB +++ • AV Comperative Advance + • AV-TEST (ochrona w 2023 na poziomie min.6) • producent systemu lub autoryzowany dystrybutor producenta musi posiadać certyfikat ISO 9001 oraz 27001 oraz **usługi związane z cyberbezpieczeństwem.**
Rozszerzone wsparcie serwisowe (należy dołączyć do oferty)	System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora do dnia 23/02/2026 r. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: • Wsparcie telefoniczne zespołu certyfikowanych inżynierów. • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. • Doradztwo w zakresie konfiguracji. • Zdalne wsparcie techniczne. • Pomoc w zakładaniu zgłoszeń serwisowych u producenta. • Przygotowanie do zdalnej konfiguracji. • Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. • Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.

	• Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. **Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w szczególności w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.** Oferent winien przedłożyć dokumenty: • Oświadczanie Producenta lub Autoryzowanego Dystrybutora producenta świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). • Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego.

Oprogramowanie do zarządzania siecią –

Oprogramowanie powinno posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami powinna być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Program powinien umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą. Moduły powinny umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program powinien wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12) i nie może być objęty limitem ilości danych, a baza danych ma być rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających powinna wymagać 64-bitowego systemu operacyjnego Windows.

Dane, które dotyczą działań pracownika na komputerze (historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp.), powinny być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej i grupowane w osobnym, dedykowanym oknie. Oprogramowanie umożliwiać ma, zgodnie z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.

Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty ma być kontrolą na poziomie wybranych Administratorów – program umożliwiać ma nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator ma mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów powinny być logowane, co oznacza, że program powinien posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów powinny być automatycznie eksportowane do zewnętrznego kolektora Syslog. Lista kont użytkowników, w tym administratorów, może być synchronizowana z Active Directory, również przez szyfrowane połączenie LDAPS.

Program powinien umożliwiać konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityka powinna pozwalać na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymuszać dostosowanie bieżących haseł do obowiązujących zasad.

Program zawierać powinien mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny powinien być wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA powinno dać się skonfigurować okres, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania powinna być pominięta wyłącznie w lokalnej konsoli serwera.

Wymaga się, aby producent oprogramowania posiadał znak jakości CYBERSECURITY MADE IN EUROPE, przyznany przez Europejską Organizację ds. Cyberbezpieczeństwa (ECSO).

Oprogramowanie powinno mieć możliwość *MONITOROWANIA INFRASTRUKTURY (BEZAGENTOWO)* obejmujące serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

✓ wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping

✓ wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)

✓ wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci

✓ wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki

✓ wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.

✓ wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku

✓ wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze

✓ wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie

✓ wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny

✓ zablokowania mapy urządzeń przed przypadkową edycją

✓ serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów

✓ serwerów pocztowych:

- program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem)
- program ma możliwość wykonywania operacji testowych
- program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa

✓ monitorowania serwerów WWW i adresów URL

✓ cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS

✓ obsługi szyfrowania SSL/TLS w powiadomieniach e-mail

✓ obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID

✓ obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych

✓ monitoringu routerów i przełączników wg:

- zmian stanu interfejsów sieciowych
- ruchu sieciowego
- podłączonych stacji roboczych – graficzna prezentacja panelu switcha
- ruchu generowanego przez podłączone do portów stacje robocze

✓ serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie

✓ wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu

✓ monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano

✓ zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny

✓ wydajności systemów Windows:
- obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.

Program powinien posiadać Inteligentne Mapy i Oddziały, służące do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzące dynamiczne mapy wg własnych filtrów (Mapy Inteligentne).

Kryteria automatycznego filtrowania dotyczyć mają m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program powinien posiadać również funkcję kompilatora plików MIB, umożliwiającego dodawanie definicji dla modułów SNMP.

Program powinien umożliwiać również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy powinny być budowane przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów powinno dać się skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji powinno dać się nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy mają pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie powinno umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0

Program powinien mieć możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

W ZAKRESIE INWENTARYZACJI program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

1. Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. Umożliwia odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
2. Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
3. Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio będzie umożliwiać audytowanie i weryfikację użytkowania licencji w organizacji.
4. Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
5. Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
6. Umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
7. Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
8. Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
9. Umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).

10. Umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji mają być logowane.
Moduł inwentaryzacji zasobów powinien umożliwiać ma prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:

✓ przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów.
✓ tworzenia powiązań między zasobami a urządzeniami,
✓ tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
✓ wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
✓ definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
✓ określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
✓ określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, masową edycję atrybutów zasobów,
✓ definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
✓ importu danych z zewnętrznego źródła (.CSV),
✓ przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., ✓ tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
✓ oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
✓ ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
✓ generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
✓ przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
✓ konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
✓ konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
✓ archiwizacji i porównywania audytów zasobów,
✓ tworzenia kodów kreskowych dla zasobów,
✓ drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
✓ inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
✓ możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
✓ inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
✓ definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z

atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”). Inwentaryzacja oprogramowania powinna zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
2. Informacje o aplikacjach używanych w organizacji.
3. Tworzenie własnych wzorców aplikacji.
4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
5. Informacje o komputerach, na których aplikacja została wykryta.
6. Zarządzanie posiadanymi licencjami.
7. Wskazywanie osób odpowiedzialnych za licencję.
8. Wskazanie użytkowników licencji.
9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili powinna być możliwość wykonania aktualnych raportów audytowych.
12. Zarządzanie posiadanymi licencjami: raport zgodności licencji.
13. Możliwość przypisania do programów numerów seryjnych, wartości itp.

Okna audytowe powinny posiadać możliwość filtrowania elementów per oddział.

W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW program powinien umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:
✓ Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
✓ Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
✓ Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
✓ Informacji o edytowanych przez użytkownika dokumentach,
✓ Historii pracy (cykliczne zrzuty ekranowe),
✓ Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),
✓ Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
✓ Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Możliwość monitorowania kosztów wydruków,
✓ Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Program ponadto powinien posiadać możliwość:

✓ wykrywania podejrzanej aktywności przez tzw. „jigglery”, mającej na celu symulowanie faktycznej pracy.
✓ zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.

✓ wyszczególnienia podejrzanej aktywności w raportach.
✓ wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności.
✓ automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności.
✓ blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone dla użytkownika lub grupy użytkowników i kopiowane lub współdzielone pomiędzy grupami lub kontami.
✓ integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.
✓ skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia.
✓ automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych.
✓ blokowania ruchu na wskazanych portach TCP/IP,
✓ blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
✓ prowadzenia rejestru naruszeń blokad
✓ wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady
✓ przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
✓ definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.

Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji powinny być tworzone dla użytkownika lub grupy użytkowników i powinny być kopiowane pomiędzy grupami lub kontami.

Program powinien posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

PROGRAM POWINIEN UMOŻLIWIAĆ REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM.
W ramach kontroli stacji użytkownika powinien być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania, czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator powinni widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu ma mieć możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu umożliwia równoczesne podłączenie do tego samego komputera kilku administratorom.

W niniejszym module ma się znajdywać baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które będą przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie pozwalać ma na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł umożliwiać ma również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawierać dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Oprogramowanie powinno umożliwiać użytkownikom monitorowanie procesu rozwiązywania

zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, wpisywane i widoczne dla obu stron. System powinien umożliwiać użycie pośredniego statusu „zgłoszenie rozwiązane" przed ostatecznym zamknięciem zgłoszenia.

Moduł ten zawierać ma również komunikator (czat), który umożliwiać ma prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów).

Ponadto czat powinien pozwalać na:
✓ zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej
✓ rozmowy również między „zwykłymi" użytkownikami
✓ przesyłanie plików między rozmówcami w trybie online
✓ tworzenie pokojów tematycznych, rozmów grupowych
✓ oznaczanie kontaktów jako „ulubionych" na liście kontaktów
✓ uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku
✓ wyświetlanie w trybie jasnym lub ciemnym.

W module zawarta ma być również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program powinien umożliwiać informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik ma mieć możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator ma możliwość tworzenia szkiców i archiwizowania komunikatów.

Dostęp do systemu zgłoszeń oraz bazy wiedzy powinien być realizowany przez dedykowany portal dostępny przez przeglądarkę internetową, wyświetlany w trybie jasnym lub ciemnym.

Funkcjonalność modułu powinna umożliwiać również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.

Moduł pomocy zdalnej powinien również umożliwiać:

✓ pobieranie listy użytkowników z Active Directory,
✓ wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym,
✓ zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
✓ zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
✓ zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń,
✓ zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy,
✓ tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,

✓ automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
✓ definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
✓ przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,
✓ procesowanie zgłoszeń użytkowników z wiadomości e-mail, eksportowania listy zgłoszeń do plików CSV i XLSX,
✓ integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,
✓ tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
✓ wykonywanie operacji na wielu zgłoszeniach równocześnie,
✓ dołączanie załączników do zgłoszeń,
✓ rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
✓ szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
✓ wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
✓ zrzuty ekranowe (podgląd pulpitu),
✓ zdalną modyfikację rejestrów,
✓ dystrybucję oprogramowania przez Agenty,
✓ definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,
✓ przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,
✓ dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
✓ zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
✓ możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
✓ możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy,
✓ planowanie nieobecności pracowników helpdesk,
✓ obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,
✓ generowanie raportów obsługi helpdesk,
✓ zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),
✓ zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
✓ wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików, bez blokowani interfejsu programu podczas przesyłania plików.

Oprogramowanie powinno mieć *MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM* poprzez blokowanie urządzeń.

1. Blokowanie urządzeń i nośników danych.
Program ma mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.

2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
9. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.
10. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
11. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
12. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:
1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.
3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:
1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
2. Podłączenie/odłączenie urządzenia przenośnego.

Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.

Definiowanie reguł monitorowanych folderów w postaci list.

Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach

nieobsługiwanych przez Agenta (np. macierze, NAS itp.)

Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.

Program umożliwiać powinien prowadzenie rejestru naruszeń blokad podłączanych nośników.

Program powinien *WSPIERAĆ ZARZĄDZANIE CZASEM I ANALIZOWANIE AKTYWNOŚCI UŻYTKOWNIKÓW* poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji powinien mieć możliwość oznaczenia sesji aktywności jako czasu prywatnego podczas wykonywania czynności prywatnych na sprzęcie firmowym. Powinien mieć również możliwość uzyskania dostępu do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni mają mieć możliwość uzyskania automatycznego dostępu do aktywności podwładnych w zespołach i indywidualnie oraz możliwość

przeanalizowania aktywności w danym okresie i uzyskania pełnego obrazu obszarów wymagających największego zaangażowania. Pracownik powinien posiadać możliwość przeglądania swoich historycznych danych, wybierając okres aktywności, który go interesuje. Zastosowane reguły mają pozwalać zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. Dostęp ma być realizowany przez przeglądarkę internetową, a strona powinna być wyświetlana w trybie jasnym lub ciemnym.

1. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.
2. Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.
3.Statystyki aktywności podwładnych widoczne dla przełożonego.
4. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.
5. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu. 6. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.
7. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.
8. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.
9. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.
10. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).
11. Wskaźnik czasu poświęconego na aktywność produktywną.
12. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.
13. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji.
14. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.

Portal informacyjny w formie platformy WWW.

Oprogramowanie posiadać powinno obszar funkcjonalny w formie platformy WWW, który pozwalać ma na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami których nazwy można zmieniać wg potrzeb.. Na każdym z dashboardów widgety powinny być rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych powinna być automatycznie odświeżana oraz:

✓ Udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem.
✓ Wyświetlana w trybie jasnym lub ciemnym (nocnym).

Oprogramowanie umożliwiać powinno zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego.

Widgety powinny prezentować dane ze wszystkich modułów funkcjonalnych oprogramowania:

✓ Mapa sieci
✓ Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci,
✓ Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów,

✓ Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW, naruszenia reguł blokad
✓ Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie,
✓ Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem), informacje o stanie Bitlocker, Windows Defender, Windows Firewall, naruszenia reguł dostępu do nośników danych,
✓ Produktywność dla grupy, Statystyki czasu nieproduktywnego.

Ochrona przed usunięciem.
Program powinien być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.

Funkcjonalność Agenta.
Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.

Inne.
Globalna wyszukiwarka, zwracająca wyniki obiektów różnego typu na podstawie wyszukiwanych słów kluczowych, np.: urządzenia, użytkownicy, zasoby, elementy interfejsu konsoli zarządzającej, elementy opcji. Program ma być dostępny w języku polskim, angielskim, bułgarskim i litewskim, wraz z Podręcznikiem Użytkownika w formie strony internetowej.

- System musi umożliwiać zarządzanie min. 35 stacjami roboczymi.

- Umowa serwisowa systemu musi być na okres min. 12 miesięcy.

Wdrożenie musi być przeprowadzone przez certyfikowanego inżyniera Wykonawcy, posiadającego aktywny certyfikat producenta, oferowanego w postępowaniu rozwiązania do zarządzania siecią i infrastrukturą IT.

Wdrożenie zostanie przeprowadzone w siedzibie Zamawiającego.