Załącznik nr 1 do Umowy

Opis Przedmiotu Zamówienia

1. **Laptop typ 1**

MINIMALNE WYMAGANIA	
LAPTOP TYP I	
Liczba sztuk	1 sztuka
Zastosowanie	Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
Przekątna ekranu	16,0 WQXGA (2560x1600), powłoką przeciwodblaskową, jasność min. 300 nits, Częstotliwość odświeżania ekranu 240Hz,
Procesor	Jednostka minimum 8-rdzeniowa / 16-wątkowa, klasy x86-64, osiągająca w teście PassMark CPU Mark wynik min. 28 000 punktów.
Pamięć RAM	32GB DDR5, dwa złącza na pamięć, możliwość rozbudowy do 64GB RAM.
Pamięć masowa	1TB SSD PCIe NVMe; Możliwość instalacji drugiego dysku PCIe
Karta graficzna	Niezintegrowana karta graficzna z min. 8GB własnej pamięci GDDR6, posiadająca wsparcie do DirectX 12, wspierająca technologię akceleracji sprzętowej CUDA, ray tracing oraz DLSS.
Klawiatura	Klawiatura odporna na zalanie (układ US), min 100 klawiszy, z wydzieloną klawiaturą numeryczną. Klawiatura podświetlana. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12.
Multimedia	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo 2x2W. Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa 1080p z diodą informującą o aktywności, trwale zainstalowana w obudowie matrycy. 1 port audio typu combo (słuchawki i mikrofon)
Łączność bezprzewodowa	Wi-Fi 6 E, 802.11ax 2x2 + Bluetooth 5.3
Bateria i zasilanie	Czas pracy na baterii min. 5 godzin pracy na baterii w teście MobileMark 2018. Zasilacz o mocy min. 230W Slim Tip
Waga i wymiary	Waga max 2.4 kg z baterią Wysokość laptopa nie większa niż 22mm.
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią. Aluminiowa pokrywa matrycy.
Certyfikaty	• Certyfikat ISO 9001, ISO 14001, ISO 50001 dla producenta sprzętu (należy załączyć do oferty) • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki. Potwierdzenie należy załączyć do oferty.
Dodatkowe oprogramowanie - w formularzu oferty należy podać pełną nazwę	Oprogramowanie zabezpieczające chroniące przed zagrożeniami, posiadające poniższe funkcjonalności: 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 możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker 83. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows. 84. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania. 85. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych. 86. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych. 87. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware. 88. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS) 89. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji. 90. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.

	91. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików. 92. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania. 93. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 94. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach. 95. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. 96. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware. 97. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora. 98. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji. 99. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji 100. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji. 101. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku. 102. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny. 103. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN 104. Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD) 105. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej. 106. Rozwiązanie pozwala na wygenerowanie pliku za pocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop). 107. Wygenerowany plik może być otwarty i wykorzystany do zdalnego podłączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji. Centralna administracja 1. Portal zarządzający jest dostępny w języku polskim. 2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej. 3. 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.

	4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. 5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów. 6. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu. 7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa. 8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV. 9. 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. 10. 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. 11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni. 12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego. 13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności. 14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki. 15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana. 16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach. 17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji. 18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email. 19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych. 20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji. 21. 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. 22. Dodanie klucza licencyjnego skutkuje aktywacją zawartości dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym. 23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego. 24. Profile mogą być przypisane do pojedynczych hostów lub do grup. 25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD. 26. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny. 27. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi. 28. 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. 29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach. 30. Pliki instalacyjne mają posiadać plików .EXE, .MSI .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent. 31. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika. 32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów. 33. 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. 34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji. 35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu. 36. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną. Dla zapewnienia wysokiego poziomu usług podmiot udzielający wsparcia technicznego dla oprogramowania musi posiadać certyfikat ISO 9001 oraz 27001 w szczególności w zakresie świadczenia usług serwisowych 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. (dokumenty załączyć do oferty).
Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. Pełna funkcjonalność systemu diagnostycznego musi być realizowana bez użycia : dostępu do sieci i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash, USBpen itp.
Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.
System operacyjny	Zainstalowany system operacyjny Windows 11 Professional lub równoważny spełniający poniższe warunki: Oferowany system musi umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.

	5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6.Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta. 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Integracja z ActiveDirectory.
Porty i złącza	Wbudowane porty i złącza: • USB 3.2 - 2 szt. • USB Typu-C (z DisplayPort) - 2 szt. • HDMI 2.1 - 1 szt. • Czytnik kart pamięci SD - 1 szt. • RJ-45 (LAN) - 1 szt. • Wyjście słuchawkowe/wejście mikrofonowe - 1 szt.

Warunki gwarancyjne, wsparcie techniczne	Min. 36 miesięcy gwarancji producenta, świadczona w trybie on-site lub door-to-door na terenie. Zachowanie dysków twardych w przypadku wystąpienia awarii

2. Laptop typ 2

MINIMALNE WYMAGANIA	
LAPTOP TYP II	
Liczba sztuk	2 sztuki
Zastosowanie	Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
Przekątna ekranu	14,5 3K (3072x1920), powłoką przeciwodblaskową, jasność min. 400 nits, Częstotliwość odświeżania ekranu 120Hz, 100% DCI-P3, Eyesafe, TÜV Low Blue Ligh
Procesor	Min. 12-rdzeniowy procesor (4 rdzenie wydajnościowe, 8 energooszczędnych), min. 16 wątków,. Architektura x86-64, wynik PassMark CPU Mark min. 26 000 punktów.
Pamięć RAM	Min. 32 GB pamięci RAM DDR5, o częstotliwości min. 5200 MHz, z możliwością rozbudowy do co najmniej 64 GB. Min. dwa sloty SO-DIMM, z czego co najmniej jeden musi być wolny.
Pamięć masowa	Min. 2 TB SSD PCIe NVMe, interfejs PCIe Gen 4.0 lub wyższy, prędkość zapisu/odczytu min. 5000 MB/s. Dysk zamontowany wewnętrznie, z możliwością wymiany.
Karta graficzna	Dedykowany układ graficzny z min. 4 GB pamięci własnej typu GDDR6, wspierający DirectX 12, OpenGL 4.6 oraz akcelerację sprzętową dla oprogramowania projektowego (np. CAD, DCC, BIM). Karta certyfikowana przez producentów oprogramowania profesjonalnego (tzw. ISV-certified).
Klawiatura	Klawiatura wyspowa, odporna na zalanie, z podświetleniem LED w kolorze białym, układ QWERTY PL. Wbudowany touchpad wielodotykowy oraz manipulator punktowy (trackpoint lub równoważny).
Multimedia	Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo 2x2W. Cyfrowy mikrofon z funkcją redukcji szumów i poprawy mowy wbudowany w obudowę matrycy. Kamera internetowa 1080p z funkcją podążania za użytkownikiem (AI tracking), trwale zainstalowana w obudowie matrycy. 1 port audio typu combo (słuchawki i mikrofon)
Łączność bezprzewodowa	Wi-Fi 6 E, 802.11ax 2x2 + Bluetooth 5.3 Opcjonalnie: gniazdo dla modemów LTE/5G z antenami (WWAN Ready).
Bateria i zasilanie	Czas pracy na baterii min. 9 godzin pracy na baterii w teście MobileMark 2018. Obsługa szybkiego ładowania – min. 50% w 30 minut. Zasilacz o mocy min. 100W Slim Tip, umożliwiający ładowanie przez USB-C lub dedykowane złącze z zabezpieczeniami przeciwprzepięciowymi.
Waga i wymiary	Waga max 1.61 kg z baterią Wysokość laptopa nie większa niż 20mm.
Obudowa	Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią. Aluminiowa pokrywa matrycy. Obudowa wykonana z materiałów o podwyższonej wytrzymałości (np. stopów metali, włókien szklanych lub kompozytów). Obudowa zgodna z normami odporności MIL-STD-810H.
Certyfikaty	Certyfikat CE, deklaracja zgodności z RoHS i REACH, system operacyjny oraz sprzęt muszą być objęte wsparciem producenta (techniczne i bezpieczeństwa). Oferowany laptop musi spełniać wymogi środowiskowe określone dla rejestracji w systemie EPEAT® na poziomie **co najmniej Gold** (zgodnie z normą EPEAT 2019 dla kategorii komputerów i monitorów). W szczególności:

	• Urządzenie musi zawierać informacje dotyczące ponownego użycia i recyklingu. • Nie może zawierać farb i powłok na dużych plastikowych częściach, które uniemożliwiają ich recykling lub ponowne użycie. • Elementy zawierające podzespoły elektroniczne oraz niebezpieczne składniki muszą być bezpiecznie i łatwo identyfikowalne oraz usuwalne. • Usunięcie materiałów i komponentów musi być możliwe zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. • Produkt musi składać się w co najmniej **65% ze składników nadających się do ponownego użycia lub recyklingu**. • Wszystkie plastikowe części o masie powyżej 25 g nie mogą zawierać więcej niż śladowych ilości środków zmniejszających palność sklasyfikowanych w Dyrektywie RE 67/548/EEC. **Weryfikacja wymogu:** Wykonawca zobowiązany jest do załączenia dokumentu (wydruku) potwierdzającego rejestrację oferowanego modelu w systemie EPEAT na poziomie co najmniej **Gold**, dostępnego na stronie: www.epeat.net.
Dodatkowe oprogramowanie - w formularzu oferty należy podać pełną nazwę	Oprogramowanie zabezpieczające chroniące przed zagrożeniami, posiadające poniższe funkcjonalności: 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 możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker 83. Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows. 84. W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania. 85. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych. 86. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych. 87. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware. 88. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS) 89. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji. 90. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji. 91. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików. 92. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania. 93. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom. 94. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach. 95. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika. 96. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware. 97. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora. 98. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji. 99. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji 100. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku,

	wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji. 101. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku. 102. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny. 103. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN 104. Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD) 105. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej. 106. Rozwiązanie pozwala na wygenerowanie pliku za pocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop). 107. Wygenerowany plik może być otwarty i wykorzystany do zdalnego podłączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji. Centralna administracja 1. Portal zarządzający jest dostępny w języku polskim. 2. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej. 3. 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. 4. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji. 5. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów. 6. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu. 7. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa. 8. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV. 9. 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. 10. 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. 11. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni. 12. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego. 13. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.

	14. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki. 15. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana. 16. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach. 17. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji. 18. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email. 19. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych. 20. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji. 21. 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. 22. Dodanie klucza licencyjnego skutkuje aktywacją zawartości dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym. 23. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego. 24. Profile mogą być przypisane do pojedynczych hostów lub do grup. 25. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD. 26. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny. 27. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi. 28. 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. 29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach. 30. Pliki instalacyjne mają posiadać plików .EXE, .MSI .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent. 31. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika. 32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów. 33. 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. 34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji. 35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu. 36. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.

	Dla zapewnienia wysokiego poziomu usług podmiot udzielający wsparcia technicznego dla oprogramowania musi posiadać certyfikat ISO 9001 oraz 27001 w szczególności w zakresie świadczenia usług serwisowych 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. (dokumenty załączyć do oferty).
Diagnostyka	System diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. Pełna funkcjonalność systemu diagnostycznego musi być realizowana bez użycia : dostępu do sieci i internetu, dysku twardego również w przypadku jego braku, urządzeń zewnętrznych i wewnętrznych typu : pamięć flash, USBpen itp.
Bezpieczeństwo	Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu powoduje uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.
System operacyjny	Zainstalowany system operacyjny Windows 11 Professional lub równoważny spełniający poniższe warunki: Oferowany system musi umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6.Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta.

	17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Integracja z ActiveDirectory.
Porty i złącza	Wbudowane porty i złącza: • USB 3.2 - 2 szt. • Thunderbolt 4 (USB 4) z Power Delivery 3.0 i DisplayPort 1.4 - 2 szt. • HDMI 2.1 - 1 szt. • Czytnik kart pamięci SD - 1 szt. • RJ-45 (LAN) - 1 szt. • Wyjście słuchawkowe/wejście mikrofonowe - 1 szt.
Warunki gwarancyjne, wsparcie techniczne	Min. 36 miesięcy gwarancji producenta, realizowana w trybie on-site lub door-to-door na terenie RP. Wykonawca zapewnia dostępność części i serwisu przez min. 5 lat od daty zakupu.
Inne wymagania	Możliwość aktualizacji BIOS/UEFI i firmware bez konieczności tworzenia konta online. Sterowniki i dokumentacja techniczna dostępne publicznie w języku polskim lub angielskim. Laptop musi umożliwiać pracę z zewnętrznymi monitorami w rozdzielczości min. 4K.

3. Stacja dokująca dla laptop typ 2

MINIMALNE WYMAGANIA	
STACJA DOKUJĄCA	
Typ	Stacja dokująca (ładowanie, obraz, dane, dźwięk)/ replikator portów
Liczba sztuk	2 sztuki
Interfejs	USB-C (Thunderbolt 4)
Obsługiwane systemy	• Windows 10 64-bit, • Windows 11 64-bit, • Linux,
Kolor	Czarny (dominujący)

Maksymalna rozdzielczość wyjściowa	• 8K – 30 Hz • 4K – 60 Hz Możliwość jednoczesnej obsługi co najmniej trzech monitorów zewnętrznych w rozdzielczości 4K (przy 60 Hz), lub jednego monitora 8K.
Ilość wspieranych monitorów	3
Zasilacz sieciowy	300W
Ładowanie (USB-C)	Możliwość zasilania podłączonego laptopa/stacji roboczej poprzez port Thunderbolt – moc zasilania minimum 230W (z czego minimum 100W przez USB-C Power Delivery).
Złącza interfejsu	• USB-C 3.2 gen 2 (1 always-on) – 4 szt. • USB 3.2 gen 1 (Thunderbolt 3, 5V, 3A)– 2 szt. • Thunderbolt (downstream) – 1 szt. • HDMI 2.1 – 1 szt. • DisplayPort 1.4– 2 szt. • RJ45(1 GB/s) – 1 szt.
Audio	Wbudowane gniazdo combo audio 3,5 mm (słuchawki/mikrofon) lub osobne wejście i wyjście audio.
Dodatkowa zawartość zestawu	• Kabel zasilający (Thunderbolt 4) – 1 szt. • Zasilacz sieciowy 300W – 1 szt.
Sterowniki i aktualizacje	Sterowniki i firmware dostępne do pobrania publicznie (bez konieczności logowania lub rejestracji), z dostępnością aktualizacji i dokumentacji w języku polskim lub angielskim.
Gwarancja	Minimum 36 miesięcy gwarancji producenta, realizowanej w trybie door-to-door lub on-site.
Certyfikaty	Deklaracja zgodności CE, zgodność z dyrektywą RoHS, REACH oraz przepisami EMC.
Bezpieczeństwo	Slot na linkę zabezpieczającą

4. Monitor 34”

MINIMALNE WYMAGANIA	
MONITOR 34”	
Liczba sztuk	12 sztuk
Typ urządzenia	Monitor panoramiczny zakrzywiony, przeznaczony do pracy biurowej, projektowej, multimedialnej i inżynierskiej, fabrycznie nowy, nieużywany, wyprodukowany nie wcześniej niż w 2024 r.
Przekątna ekranu	Minimum 34 cale (86,7 cm) w układzie panoramicznym. Zakrzywiony ekran o promieniu zakrzywienia max. 1900R.
Rozdzielczość	Minimum 3440 × 1440 pikseli (WQHD), proporcje ekranu 21:9.
Częstotliwość odświeżania	Minimum 120 Hz.
Technologia matrycy	Matryca typu IPS Black z podświetleniem LED Edgelight, kąt widzenia 178°/178°, kontrast statyczny min. 2000:1, powłoka przeciwodblaskowa z twardością min. 3H.
Jasność	Minimum 300 cd/m² (typowa).
Czas reakcji	Maksymalnie 8 ms (normalny) i 5 ms (tryb szybki).
Kolorystyka i odwzorowanie	Obsługa co najmniej: 98% DCI-P3, 98% Display P3, 100% sRGB i 100% BT.709. Wyświetlanie min. 1,07 mld kolorów (technologia 8-bit + FRC). Średnia wartość Delta E < 2.
Ergonomia	Regulacja wysokości min. 150 mm, pochylenie od -5° do +21°, obrót lewo/prawo min. ±30°. Standard VESA 100×100 mm. W zestawie stopka i podstawka monitora.
Złącza sygnałowe	Min. 1 x HDMI (HDCP 1.4/2.2), 1 x DisplayPort 1.4 (HDCP 1.4/2.2), 1 x Thunderbolt 4 upstream (zasilanie i wideo, do 90W), 1 x Thunderbolt 4 downstream (15W), 1 x USB-C upstream (dane). Obsługa daisy-chain i alternatywnego trybu DisplayPort.

Złącza USB	Min. 4 x USB-A (10 Gbps), min. 2 x USB-C (10 Gbps, 15W), 1 x USB-A quick access z funkcją ładowania, USB-C downstream do akcesoriów.
Sieć i KVM	Wbudowana karta sieciowa 2.5 GbE z funkcjami PXE Boot, MAC Address Pass-Through i Wake on LAN. Wsparcie dla funkcji KVM (przełączania klawiatury, wideo i myszy) oraz PBP / PIP (dzielony ekran).
Wbudowane audio	Wbudowane głośniki stereo – min. 2 x 5 W oraz wyjście liniowe audio 3,5 mm (line-out).
Czujniki i komfort wzroku	Wbudowany czujnik światła otoczenia (regulacja jasności i temperatury barwowej), tryb redukcji niebieskiego światła (Low Blue Light <35%), certyfikat ergonomii wzroku min. TÜV Rheinland Eye Comfort 5*.
Funkcje zarządzania	Kompatybilność z aplikacjami do zarządzania IT (np. SCCM, InTune), wbudowane funkcje kalibracji sprzętowej, możliwość zapisania presetów kolorów (ICC). Obsługa Easy Arrange (do 48 układów okien), iMST – wewnętrzne dzielenie ekranu bez splittera.
Energooszczędność	Certyfikaty Energy Star, EPEAT Gold z oznaczeniem Climate+, TCO Certified, wsparcie dla funkcji PowerNap, zużycie energii: ≤30W (typowo), ≤0.5W (standby).
Wymiary i waga	Wysokość z podstawą nie przekraczająca wymiary: 392,8–542,8 mm, szerokość: 813,5 mm, głębokość: 240 mm, waga z podstawą: max. 11 kg, bez podstawy: max. 8 kg.
Zabezpieczenia fizyczne	Złącze zabezpieczenia fizycznego (blokada typu Kensington Lock oraz blokada podstawy).
Zgodność i standardy	Zgodność z normami CE, RoHS, REACH, TCO Edge, bez użycia rtęci i arsenu, wykonany z materiałów z recyklingu (min. 85% plastików PCR, 50% stali, 20% szkła). Opakowanie z materiałów odnawialnych, nadające się do recyklingu.
Gwarancja	Min. 36 miesięcy gwarancji producenta typu Wsparcie producenta w języku polskim.

5. Macierz NAS

MINIMALNE WYMAGANIA	
MACIERZ NAS	
Procesor	Wielordzeniowy procesor osiągający wynik minimum 4 tys. punktów w teście PassMark.
Obudowa	Typu desktop (wolnostojąca).
Pamięć RAM	Minimum 4GB DDR4 ECC.
Interfejsy sieciowe	Minimum 4 porty 1GbE RJ-45 z obsługą agregacji łączy.
Ilość obsługiwanych dysków	Minimum 6 dysków o maksymalnej pojemności nie mniejszej niż 18TB każdy, po podłączeniu modułów rozszerzających minimum 16 dysków.
Wskaźniki LED	Status, HDD 1-6, zasilanie, LAN 1-4
Obsługa RAID	RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare.
Funkcje RAID	Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5.
Szyfrowanie	Możliwość szyfrowania wybranych udziałów sieciowych.
Protokoły	SMB, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	1. Serwer VPN, Serwer pocztowy, Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów.

	2. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 7 lub nowszym według harmonogramu z centralnej konsoli zarządzania dostępnej lokalnie oraz zdalnie, z możliwością przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Bez ograniczenia liczby podłączanych komputerów do systemu kopii zapasowej. 3. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora.
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów.
System plików	Dyski wewnętrzne: BTRFS. Dyski zewnętrzne: FAT, NTFS, EXT3, EXT4, HFS+.
Język GUI	Polski
Gwarancja i serwis	Minimum 36 miesięcy gwarancji świadczonej przez autoryzowany serwis producenta działającej w trybie 5/13 NBD On-site na cały system złożony z serwera, dysków i akcesoriów z opcją pozostawienia uszkodzonego nośnika u Zgłaszającego i gwarantowanym terminem realizacji naprawy na następny dzień roboczy.
Typowy pobór mocy podczas pracy	Maksymalnie 80W
Certyfikaty	CE, FCC
Zasilanie	Zasilacz wewnętrzny o mocy minimum 200W.
Dodatkowe Wsparcie techniczne	**Zakres dodatkowego wsparcia** Wsparcie techniczne musi być świadczone przez wykwalifikowanych inżynierów Producenta oferowanego rozwiązania lub certyfikowanych inżynierów dystrybutora oferowanego rozwiązania na terenie Polski posiadającego autoryzację producenta od minimum 10 lat. Wymagane jest, aby osoby te posiadały odpowiednie kompetencje techniczne i doświadczenie w obsłudze oraz serwisowaniu urządzeń objętych niniejszą dostawą, co zapewni najwyższy poziom jakości usług oraz bezpieczeństwo danych Zamawiającego. 1. **Proaktywne monitorowanie infrastruktury** o Ciągłe monitorowanie pracy urządzeń, obejmujące: ▪ Stan techniczny nośników danych, w tym parametry SMART, zużycie i temperaturę. ▪ Wykorzystanie zasobów systemowych, takich jak procesor, pamięć i przestrzeń dyskowa. ▪ Analizę logów systemowych pod kątem potencjalnych zagrożeń i anomalii. o Automatyczne powiadomienia o wykrytych problemach technicznych przesyłane do administratora Zamawiającego oraz zespołu wsparcia. 2. **Kwartalne raportowanie stanu infrastruktury** o Przygotowywanie szczegółowych raportów technicznych zawierających: ▪ Stan urządzeń, w tym status macierzy dyskowych oraz aktualną konfigurację systemową. ▪ Wykorzystanie zasobów i ich dynamikę w okresie sprawozdawczym. ▪ Informacje o liczbie zgłoszeń serwisowych, podejmowanych działaniach oraz ich wynikach. ▪ Rekomendacje dotyczące optymalizacji wydajności i planowania przyszłych działań.

	○ Raporty dostarczane w formie elektronicznej oraz omawiane podczas cyklicznych spotkań technicznych z przedstawicielami Zamawiającego. 3. **Reakcja serwisowa i wsparcie w sytuacjach krytycznych** ○ Gwarantowany czas reakcji na zgłoszenia: ▪ Krytyczne awarie: **maksymalnie 1 godzina** od zgłoszenia. ▪ Problemy o wysokim priorytecie: **do 4 godzin roboczych**. ▪ Problemy o niskim priorytecie: **do 1 dnia roboczego**. 4. **Przeglądy techniczne i diagnostyka** ○ Realizacja kwartalnych przeglądów technicznych obejmujących: ▪ Weryfikację stanu nośników danych i macierzy RAID. ▪ Aktualizację systemów operacyjnych oraz aplikacji zainstalowanych na urządzeniach. ▪ Testowanie procedur odzyskiwania danych z kopii zapasowych. ▪ Sprawdzanie konfiguracji systemów zabezpieczeń oraz logów w celu identyfikacji potencjalnych zagrożeń. ○ Każdy przegląd kończy się sporządzeniem szczegółowego raportu dla Zamawiającego wraz z rekomendacjami. 5. **Analiza ryzyk i doradztwo techniczne** ○ Regularne identyfikowanie potencjalnych zagrożeń dla działania urządzeń oraz opracowanie planów zapobiegawczych. ○ Bieżąca analiza wydajności oraz analiza ryzyk związanych z przetwarzaniem danych. ○ Proponowanie działań optymalizacyjnych, dostosowanych do zmieniających się potrzeb Zamawiającego. 6. **Wsparcie w integracji i optymalizacji infrastruktury** ○ Pomoc techniczna przy integracji urządzeń z istniejącą infrastrukturą sieciową i systemami informatycznymi Zamawiającego. ○ Konfiguracja i utrzymanie mechanizmów zabezpieczeń danych, w tym systemów tworzenia kopii zapasowych oraz ich odtwarzania. Dostosowanie konfiguracji urządzeń do zmieniających się wymagań operacyjnych, zapewniające optymalne wykorzystanie zasobów **Oferent winien przedłożyć dokumenty:** Dokument potwierdzony przez Producenta lub Autoryzowanego Dystrybutora producenta o gotowości świadczenia na rzecz Zamawiającego wymaganego wsparcia (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej

6. Dysk NAS

MINIMALNE WYMAGANIA	
DYSK NAS	
Liczba sztuk	4 sztuki
Pojemność	20 TB
Interfejs	SATA 6 Gb/s
Technologia nagrywania	CMR
Konstrukcja dysku	Hel
Limit obciążenia pracą (WRL)	550
Czujniki drgań ruchu obrotowego (RV)	Tak

Pamięć podręczna	512MB
Średni czas bezawaryjnej pracy (MTBF)	2500000h
Nieodwracalne błędy odczytu na odczytane bity	Maksymalnie 1 na 10E15
Godziny pracy	8 760 rocznie
Wielkość sektora (liczba bajtów na sektor logiczny)	512E
Rescue Data Recovery Services	3 lata
Okres ograniczonej gwarancji	5 lat
Prędkość obrotowa	7200 obr./min
Szybkość interfejsu	6.0, 3.0, 1.5 Gb/s
Maksymalna średnia szybkość transmisji	285 MB/s
Drgania przy częstotliwości 10-1500 Hz	12,5 rad/s
Typowy prąd rozruchu	2.0 A
Średni pobór mocy podczas pracy	7,7 W
Średni typowy pobór mocy w trybie gotowości	1,2 W
Średni typowy pobór mocy w trybie uśpienia	1,2 W
Wibracje (w stanie spoczynku: 10 Hz do 500 Hz)	2,27 Grms
Akustyka, tryb bezczynności	20 dBA
Akustyka, podczas wyszukiwania	26 dBA
Odporność na wstrząsy podczas pracy	40/40 G, przy założeniu 2 ms w trybie odczytu/zapisu
Waga	670 g