Komputer przenośny (laptop) – 277 sztuk

Szczegółowy opis		
Komputer przenośny. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy (numer konfiguracji lub part numer) oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. Jeśli na stronie internetowej producenta nie jest dostępna pełna oferta modeli sprzętu wraz z jego konfiguracją, do oferty należy dołączyć katalog producenta zaoferowanego produktu umożliwiający weryfikację oferty pod kątem zgodności z wymaganiami Zamawiającego. Nie dopuszcza się zaoferowania komputera refurbished.		
Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający.		
Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu z wymogami niniejszej SWZ. W tym celu Wykonawcy na wezwanie Zamawiającego dostarczą do siedziby Zamawiającego w terminie 5 dni od daty otrzymania wezwania, próbkę oferowanego sprzętu. W odniesieniu do programowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Ocena złożonych próbek zostanie dokonana przez Komisję Przetargową na zasadzie spełnia / nie spełnia. Z badania każdej próbki zostanie sporządzony protokół. Pozytywna ocena próbki będzie oznaczała zgodność próbki (oferty) z treścią SWZ. Niezgodność próbki z SWZ chociażby w zakresie jednego parametru podlegającemu badaniu bądź nieprzedłożenie wymaganej próbki w sposób i terminie wymaganym przez Zamawiającego będzie oznaczało negatywny wynik oceny próbki i będzie skutkowało odrzuceniem oferty.		
Zamawiający zastrzega sobie prawo do sprawdzenia reżimu gwarancyjnego producenta oraz dostarczonej konfiguracji na dedykowanej stronie internetowej producenta sprzętu.		
Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne komputerów**
1.	Procesor	Procesor klasy x86, zaprojektowany do pracy w komputerach przenośnych, zapewniający wydajność całego oferowanego laptopa Overall Rating min 1050 pkt w teście SYSmark® 25 w oparciu o wyniki testów dostarczone wyniki wykonanych testów w PDF.
2.	Pamięć operacyjna RAM	Min 8GB, rodzaj pamięci DDR4 min. 3200MHz.
3.	Parametry pamięci masowej	Min 256GB SSD NVMe, zawierający RECOVERY umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Możliwość rozbudowy do konfiguracji dwudyskowej w oparciu o dysk M.2 SSD oraz 2,5”. Dopuszcza się również rozwiązania posiadające 2 złącza M.2 dla dysków SSD. W przypadku 2,5” gotowa do rozbudowy zatoka umożliwiająca podłączenie dysku.
4.	Karta graficzna	Zintegrowana

5.	Wyposażenie multimedialne	Wbudowana karta dźwiękowa zgodna z HD Audio, wbudowane głośniki stereo Dolby Audio min 2x1.5W, wbudowany mikrofon, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), wbudowana kamera internetowa z mechaniczną przesłoną.
6.	Obudowa	Obudowa wyposażona w zawiasy metalowe. Nie dopuszcza się demontowalnych zasłon kamery. Kąt otwarcia matrycy min. 176 stopni. W obudowę wbudowane co najmniej 2 diody sygnalizujące stan naładowania akumulatora oraz pracę dysku twardego lub stan pracy komputera.
7.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w interfejs SATA III (6 Gb/s) do obsługi dysków twardych. Płyta główna i konstrukcja laptopa wspierająca konfiguracje dwu dyskową SSD M.2+ HDD 2,5''.
8.	Zgodność z systemami operacyjnymi	Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera).
9.	Bezpieczeństwo	Backup i przywracanie danych - Deduplikacja danych na źródle, - Backup przyrostowy i różnicowy, - Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji, - Backup danych lokalnych – plikowy oraz poczty Outlook, - Backup otwartych plików (VSS), - Filtr plików oraz folderów, - Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.), - Wyłączanie komputera po wykonaniu backupu, - Przywracanie danych do wskazanej lokalizacji, - Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora, - Wyszukiwanie plików w repozytorium użytkownika, Ustawienia - Automatyczne logowanie, - Zapamiętywanie danych logowania, - Automatyczne uruchamianie programu przy starcie systemu, - Ustawianie priorytetu dla procesu backupu, - Zmiana klucza szyfrującego, - Ustawienia przepustowości/zajętości pasma, - Konfiguracja wydajności procesu backupu,

		Bezpieczeństwo - Zastępowanie nazwy pliku GUID-em, - Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika, - Kompresja danych, - Transmisja po bezpiecznym protokole TLS, - Deklaracja klucza szyfrującego dane użytkownika, - Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji, - Obliczanie sumy kontrolnej, - Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski. WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze, Mac OS, Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Licencja obowiązuje przez okres minimum 24 miesiące Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji Zintegrowany układ TPM2.0
10.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
11.	BIOS	BIOS zgodny ze specyfikacją UEFI. Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji: - wersji BIOS - nr seryjnym komputera - ilości pamięci RAM - typie procesora - zainstalowanym dysku - o zintegrowanej w BIOS licencji na system operacyjny - odczytania z BIOS nazwy producenta komputera oraz modelu lub konfiguracji zaoferowanej jednostki. Nie dopuszcza się wykorzystania pól Asset TAG w BIOS do propagacji w/w informacji Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:

		Możliwość ustawienia: - hasła dla twardego dysku - hasła Administratora oraz Użytkownika - kolejności bootowania - włączania/wyłączania WiFi - włączania/wyłączania wirtualizacji - włączania/wyłączania wgrania starszej wersji BIOS - sposobu działania klawiszy F1-F12 (normalna praca/skróty) - trybu wydajności lub chłodzenia W przypadku występowania na klawiaturze przycisku Fn wymaga się funkcjonalności w BIOS umożliwiającej zamianę funkcji pomiędzy klawiszami Ctrl i Fn, tak aby użytkownik nie musiał zmieniać swoich przyzwyczajeń umiejscowienia przycisków Ctrl i Fn, co wpływa na komfort obsługi. Przy ustawionym haśle Administratora, zalogowany Użytkownik do BIOS musi mieć możliwość zmiany własnego hasła. Nie dopuszcza się możliwości edycji ustawień wpływających na bezpieczeństwo urządzenia. Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.
12.	Ekran	Matryca 15,6” z podświetleniem w technologii LED, powłoka antyrefleksyjna Anti-Glare, rozdzielczość: FHD 1920x1080, jasność min. 250nits.
13.	Interfejsy / Komunikacja	Minimum: 2x USB typ-A w tym min. 1 w standardzie 3.2 1x USB typ-C w tym min. 1 w standardzie 3.2 1x HDMI 1.4 1x złącze słuchawkowe i złącze mikrofonu 1x zintegrowane z płytą główną, wbudowane w komputer złącze RJ-45 100/1000Mbps

		Złącze HDMI musi umożliwiać podłączenie i obsługę zewnętrznego wyświetlacza w rozdzielczości min. 3840x2160 przy min. 30Hz.
14.	Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AC 2x2 Wbudowana karta Bluetooth 5.0
15.	Klawiatura	Klawiatura, układ QWERTY US lub QWERTY EU, odporna na zalanie. Klawiatura z wydzielonym blokiem numerycznym.
16.	Wbudowany akumulator	Pozwalający na nieprzerwaną pracę urządzenia przez min. 8 godziny. Wyniki muszą być potwierdzone MobileMark 25. Zamawiający wymaga załączenia wyników testów w formacie PDF dołączonych do oferty
17.	Zasilacz	Zasilacz zewnętrzny o mocy minimum 60W Zasilacz wyprodukowany przez producenta komputera lub na jego zlecenie.
18.	Certyfikaty, oświadczenia i standardy	- Certyfikat ISO 9001 dla producenta sprzętu (należy załączyć do oferty) - Certyfikat ISO 50001 dla producenta sprzętu (należy załączyć do oferty) - Deklaracja zgodności CE (załączyć do oferty)
19.	Waga	Waga urządzenia z baterią podstawową poniżej 1.7kg
20.	System operacyjny	**Microsoft Windows 10 Home 64 bit** lub równoważny. Zamawiający nie dopuszcza licencji typu refurbished lub wersji edukacyjnych (EDU / Acdmc / STF) Za równoważny Zamawiający przyjmie system klasy PC spełniający opis równoważności 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 tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 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 – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 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. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."

		24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 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. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach

		42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń Licencja systemu operacyjnego zaimplementowana w BIOS komputera, umożliwiająca instalację systemu bez podawania klucza oraz bez aktywacji systemu za pośrednictwem Internetu. Nie dopuszcza się zaoferowania systemu operacyjnego typu refurbished.
21.	Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.
22.	Gwarancja	Minimalny czas trwania gwarancji producenta wynosi 2 lata, świadczona w standardzie wysyłkowym (na koszt Wykonawcy, producenta lub autoryzowanego punktu serwisowego).
23.	Wsparcie techniczne producenta	▪ Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera ▪ Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00 Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta. Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.
24.	Konfiguracja wstępna	Zamawiający wymaga przeprowadzenia konfiguracji wstępnej komputera przez co rozumie się: • Przeprowadzenie pierwszego uruchomienia komputera • Utworzenie konta użytkownika lokalnego • Zainstalowanie aktualizacji systemu operacyjnego do najnowszej wersji Windows Home 11 64 bit (dopuszcza się aktualizację nie starsze niż 4 tygodnie przed dostawą sprzętu do zamawiającego) • Instalacja oprogramowania biurowego • Instalacja przeglądarki Google Chrome

25.	Oprogramowanie biurowe	Przedmiotem zamówienia jest dostawa oprogramowania biurowego w postaci nie mniej niż 12-miesięcznej subskrypcji 277 licencji oprogramowania Microsoft Office 365 Personal w skład którego wchodzą Word, Excel, PowerPoint, OneNote, Outlook, Publisher i Access lub oprogramowania równoważnego (zwanego również „Usługą"), udostępnienie oprogramowania drogą elektroniczną poprzez dostęp do strony internetowej zawierającej dane oprogramowanie oraz dokument potwierdzający prawo do korzystania z programu na wymaganej liczbie stanowisk roboczych wraz z danymi zawierającymi informację umożliwiającą instalację wraz ze wsparciem oprogramowania przez okres subskrypcji. Minimalne warunki równoważności: Zintegrowany pakiet biurowy (zawierający co najmniej: edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji, program do obsługi poczty elektronicznej oraz kalendarza) charakteryzujący się następującymi cechami: 1. Możliwość automatycznej instalacji komponentów (przy użyciu instalatora systemowego). 2. Możliwość zdalnej instalacji komponentów. 3. Możliwość instalacji wszystkich składników pakietu na komputerze (wykluczenie produktów działających w chmurze). 4. Całkowicie zlokalizowany w języku polskim system komunikatów i podręcznej pomocy technicznej w pakiecie. 5. Możliwość prowadzenia dyskusji i subskrypcji dokumentów w sieci z automatycznym powiadomieniem o zmianach w dokumentach. 6. W systemach pocztowych - możliwość delegacji uprawnień do otwierania, drukowania, modyfikowania i czytania załączanych dokumentów i informacji. 7. Współpraca z systemem MS Exchange, w tym odbiór poczty, możliwość udostępniania kalendarza dla innych użytkowników. 8. Możliwość blokowania niebezpiecznej lub niechcianej poczty. 9. Wsparcie dla formatu XML w podstawowych aplikacjach. 10. Możliwość nadawania uprawnień do modyfikacji i formatowania dokumentów lub ich fragmentów. 11. Automatyczne przesyłanie poczty na podstawie reguł, automatyczne odpowiedzi. 12. Automatyczne wypisywanie hyperlinków,

		13. Możliwość automatycznego odświeżania danych pochodzących z Internetu w arkuszach kalkulacyjnych. 14. Możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów cyfrowych, pozwalających na stwierdzenie czy dany dokument/arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony. 15. Możliwość automatycznego odzyskiwania dokumentów i arkuszy kalkulacyjnych w wypadku odcięcia dopływu prądu. 16. Licencja roczna. 17. Licencja musi zawierać w sobie dostęp do zdalnej chmury o pojemności nie mniej niż 1TB dla użytkownika. Dane w chmurze muszą przechowywane być w sposób bezpieczny, uniemożliwiający dostęp do nich przez osoby niepowołane. 18. Prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: *.DOC, *.DOCX, *.XLS, *.XLSX, w tym obsługa formatowania, makr, formuł, formularzy w plikach wytworzonych w MS Office 2007, MS Office 2010, MS Office 2013, MS Office 2016. UWAGA: Zaoferowane oprogramowanie musi posiadać taki sposób licencjonowania, który zapewni jego instalację na komputerze (komputerach) Koszt zaoferowanych licencji na oprogramowanie musi uwzględniać całkowity koszt ich wykorzystania.
26.	Oprogramowanie antywirusowe	Wymagania dotyczące system ochrony anty wirusowej z zaporą ogniową dla stacji roboczych – okres subskrypcji nie mniej niż 24 m-ce o poniższych minimalnych parametrach . 1. Ochrona antywirusowa stacji roboczych: - Microsoft Windows 7 (32-bit i 64-bit) - Microsoft Windows 8.1 (32-bit i 64-bit) - Microsoft Windows 10 (32-bit i 64-bit) - Microsoft Windows 11 (32-bit i 64-bit) 2. Ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli. 3. Możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach. 4. Polski interfejs użytkownika aplikacji ochronnej.

		Wymagania dotyczące technologii: 1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy. 2. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane. 3. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan". 4. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie pliku offline ze strony producenta i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu. 5. Możliwość wywołania skanowania komputera na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta. 6. Możliwość wywołania skanowania komputera w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera. 7. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika. 8. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie. 9. 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). 10. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe. 11. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów. 12. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów. 13. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit". 14. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie. 15. Ochrona pliku 'hosts' przed niepożądanymi wpisami. 16. Mechanizm centralnego zarządzania elementami kwarantanny znajdującymi się na stacjach klienckich. 17. Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona.

		18. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda. 19. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX. 20. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa. 21. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji. 22. Automatyczne uruchamianie procedur naprawczych. 23. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione. 24. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365). 25. Automatyczne powiadomienie użytkowników oraz administratora o wykrytych zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona. 26. Możliwość zablokowania wychodzącej wiadomości e-mail, jeżeli zostanie w niej wykryty zainfekowany załącznik. 27. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http. 28. Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http. 29. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta. 30. Automatyczna kwarantanna blokująca ruch przychodzący i wychodzący, włączająca się w momencie, gdy stacja robocza posiada stare sygnatury antywirusowe. 31. Wsparcie dla technologii Microsoft Network Access Protection (NAP). 32. Ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX i pobieranych plików. 33. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie *Network Interceptor Framework* (niezależnie od rodzaju i wersji przeglądarki). 34. Możliwość zabezpieczenia połączenia do witryn skategoryzowanych przez producenta, jako ‘bankowość elektroniczna’ poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z bankiem. 35. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z daną witryną HTTPS. 36. Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez producenta. 37. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji. 38. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.

		39. Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych. 40. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej. 41. Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej) 42. Brak konieczności restartu komputera po zainstalowaniu aplikacji w środowisku Windows 43. Moduł kontroli urządzeń zapewniający możliwość zezwolenia lub zablokowania dostępu do urządzeń zewnętrznych (np. napędy USB, urządzenia bluetooth, czytniki kart pamięci, napędy CD/DVD, stacje dyskietek). 44. Moduł kontroli urządzeń zarządzany z poziomu konsoli centralnego zarządzania. 45. Moduł kontroli urządzeń umożliwia dodanie 'zaufanego urządzenia' poprzez podanie jego identyfikatora sprzętowego. Wymagania dotyczące systemu zarządzania centralnego: 1. System centralnego zarządzania może być zainstalowany na wersjach serwerowych Microsoft Windows oraz Linux. 2. Instalacja sytemu centralnego zarządzania dla Microsoft Windows musi wspierać następujące wersje systemów operacyjnych: - Windows Server 2008 SP1 64-bit: Standard, Enterprise, Web Server, Small Business Server, Essential Business Server - Windows Server 2008 R2: Standard, Enterprise, Web Server - Windows Server 2012: Essentials, Standard, Datacenter - Windows Server 2012 R2: Essentials, Standard, Datacenter - Windows Server 2016; Essentials, Standard or Datacenter editions - Windows Server 2019; Essentials, Standard or Datacenter editions 3. Instalacja sytemu centralnego zarządzania dla Linux musi wspierać następujące wersje systemów operacyjnych: - Red Hat Enterprise Linux 6,7,8 64-bit - CentOS 6,7,8 64-bit - SuSE Linux Enterprise Server 11,12,15 64-bit - SuSE Linux Enterprise Desktop 11,12,15 64-bit - openSUSE Leap 43,15 64-bit - Debian GNU Linux 8,9 64-bit - Ubuntu 14.04,16.04,18.04 64-bit 4. Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI) i JAR lub też bezpośrednią instalację zdalną nienadzorowaną.

		5. Narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nowe wersję. 6. Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem). 7. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi. 8. Pełne centralne zarządzanie dla środowisk Windows Server 2003 (32-bit oraz 64-bit), Windows Server 2008 (32-bit oraz 64-bit), Windows Server 2008 R2, Windows Server 2012, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Linux. 9. Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta. 10. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa. 11. Centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy. 12. Możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów). 13. Tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach. 14. Możliwość importu struktury drzewa z Microsoft Active Directory. 15. Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników. 16. Możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający. 17. Możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji. 18. Możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta. 19. Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania. 20. Dane muszą być przesyłane do serwera zarządzania podczas kolejnego połączenia. 21. Możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich. 22. Umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe.

		23. Automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych (min. 3 inne) podczas instalacji. 24. Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej, niż co 7 dni (zalecane codzienne aktualizacje). 25. Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe. 26. Możliwość eksportu raportów z pracy systemu do pliku HTML. 27. Możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich. 28. Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”. 29. Program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa. 30. Program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe. 31. Program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy). 32. Program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów. 33. Dedykowany system raportowania dostępny przez przeglądarkę internetową umożliwiający podgląd statystyk dotyczących wykrytych wirusów, przeprowadzonych ataków, zainstalowanego oprogramowania oraz statystyk połączenia stacji klienckich. 34. System raportowania umożliwiający wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora. 35. Zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania. 36. Możliwość przekierowania alertów bezpośrednio do serwera Syslog. 37. Możliwość tworzenia wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw). 38. System umożliwiający wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączania programu. 39. Pełna kopia bazy danych systemu zarządzania centralnego może być wykonywana automatycznie zgodnie z harmonogramem określonym przez administratora. 40. Administrator ma możliwość określenia liczby kopii bazy danych, jaka będzie przetrzymywana.