

## Załącznik nr 1 do zapytania ofertowego

### SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

#### Komputer typu laptop – 1 szt.

Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.	
Ekran	15.6" LED IPS FHD o rozdzielczości 1920x1080, z powłoką matową, nie dopuszcza się matryc typu "glare".
Wydajność komputera	<p>Oferowany komputer przenośny musi osiągać w teście wydajności :</p> <p>SYSMARK 25 – wynik min. 1200 – test z przeprowadzonej konfiguracji załączyć na wezwanie Zamawiającego.</p> <p>Wymagane testy wydajnościowe wykonawca musi przeprowadzić na automatycznych ustawieniach konfiguratora dołączonego przez firmę BAPCO i przy natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowanie overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS ( tzn. wyłączanie urządzeń stanowiących pełną konfigurację) jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.).</p> <p>Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych wszystkich wymaganych testów Oferent musi dostarczyć Zamawiającemu oprogramowanie testujące, komputer do testu oraz dokładny opis metodyki przeprowadzonego testu wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego</p>
Chipset	Zaprojektowany i wykonany do pracy w komputerach przenośnych rekomendowany przez producenta procesora.
Obudowa	Dopuszczalne kolory – czarny/srebrny.
Pamięć RAM	minimum 16GB DDR4 (pamięć RAM rozszerzalna do 32GB – nie dopuszcza się wlotowanych pamięci w płytę główną).
Dysk twardy	<p>minimum 512GB SSD</p> <p>Dysk twardy musi zawierać partycję recovery – na partycji musi znajdować się obraz zainstalowanych i skonfigurowanych elementów tj.:</p>

	<ul style="list-style-type: none"> <li>- systemu operacyjnego</li> <li>- oprogramowania antywirusowego</li> </ul> <p>Partycja musi zapewniać przywrócenie systemu operacyjnego, zainstalowanego i skonfigurowanego w/w oprogramowania.</p> <p>Możliwość instalacji wewnątrz obudowy drugiego dysku 2.5.</p>
Karta graficzna	Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem DirectX 12, OpenGL 4.5, pamięć współdzielona z pamięcią RAM, dynamicznie przydzielana.
Karta dźwiękowa	Karta dźwiękowa zgodna z HD Audio, wbudowane dwa głośniki stereo oraz dwa cyfrowe mikrofony
Wbudowane połączenia i karty sieciowe	Karta sieciowa LAN 10/100/1000 LAN WLAN 802.11 ax wraz z Bluetooth 5.0
Porty/złącza (wbudowane)	<ul style="list-style-type: none"> <li>1x Złącze RJ-45 (podłączenie sieci lokalnej)</li> <li>1x Czytnik Kart pamięci SD</li> <li>2x USB 3.2</li> <li>1x USB 2.0</li> <li>1x VGA</li> <li>1x Gniazdo mikrofonowe/Gniazdo słuchawkowe (Combo)</li> <li>1x HDMI ze wsparciem HDCP</li> <li>1x zasilanie DC-in</li> </ul>
Klawiatura	Pełnowymiarowa klawiatura podświetlana z wydzielonymi pełnowymiarowymi klawiszami numerycznymi w prawej części klawiatury, w układzie US-QWERTY, polskie znaki zgodne z układem MS Windows "polski programistyczny", klawiatura podświetlana musi być wyposażona w 2 klawisze ALT (prawy i lewy).
Urządzenie wskazujące	Touch Pad (płytką dotykowa) wbudowana w obudowę notebooka.  Czytnik linii papilarnych
Kamera	Wbudowana, o parametrach:  HD 1280x720, 720p HD audio/video nagrywanie. Wbudowane dwa kierunkowe mikrofony.  Mechaniczna przesłona kamery.
Bateria	4-ogniowa wbudowana bateria polimerowa 54 Wh z funkcją

	ExpressCharge™
Zasilacz	Zewnętrzny, pracujący w sieci elektrycznej 230V 50/60Hz, max 90W.
Obudowa waga i wymiary	<p>Waga nie większa niż 1,8kg, grubość nie przekraczająca 20mm. Obudowa wzmocniona, szkielet wykonany ze wzmocnionego aluminium.</p> <p>Obudowa musi spełniać standard MIL-STD 810G (potwierdzony w oficjalnych dokumentach producenta lub załączonym wynikiem z przeprowadzonych testów)</p>
Bezpieczeństwo	<ul style="list-style-type: none"> <li>- Zabezpieczenie BIOS hasłem użytkownika.</li> <li>- Zabezpieczenie dysku twardego hasłem użytkownika.</li> <li>- Złącze typu Kensington Lock.</li> <li>- Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego - Trusted Platform Module 2.0.</li> </ul>
Gwarancja	<p>Gwarancja producenta komputera minimum 36 miesięcy</p> <p>Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – wymagane oświadczenie potwierdzające, że serwis będzie realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego producenta (oświadczenie należy złożyć na żądanie Zamawiającego).</p> <p>Autoryzowany Partner Serwisowy musi posiadać status autoryzowanego partnera serwisowego producenta komputera.</p> <p>Serwis urządzeń musi być realizowany zgodnie z wymogami normy ISO9001</p> <p>Wymagane okno czasowe dla zgłaszania usterek min. wszystkie dni robocze w godzinach od 8:00 do 20:00. Zgłoszenie serwisowe przyjmowane poprzez stronę www lub telefonicznie (dedykowany numer serwisowy do obsługi zgłoszeń serwisowych).</p>
System operacyjny – w formularzu oferty należy podać pełną nazwę oferowanego	<p>System operacyjny Windows 11 Professional lub równoważny, musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:</p> <ol style="list-style-type: none"> <li>1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:</li> </ol>

oprogramowania	<ol style="list-style-type: none"><li>a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,</li><li>b. Dotykowy umożliwiający sterowanie dotykaniem na urządzeniach typu tablet lub monitorach dotykowych</li></ol> <ol style="list-style-type: none"><li>2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego</li><li>3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim</li><li>4. Możliwość tworzenia pulpitu wirtualnych, przenoszenia aplikacji pomiędzy pulpitem i przełączanie się pomiędzy pulpitem za pomocą skrótów klawiaturowych lub GUI.</li><li>5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe</li><li>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,</li><li>7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.</li><li>8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim</li><li>9. Wbudowany system pomocy w języku polskim.</li><li>10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).</li><li>11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.</li><li>12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.</li><li>13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.</li><li>14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.</li></ol>
----------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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:
- Login i hasło,
  - Karty inteligentne i certyfikaty (smartcard),
  - Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
  - Certyfikat/Klucz i PIN
  - 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

	<p>środowiskach</p> <p>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń</p> <p>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń</p>
Certyfikaty i standardy	<p>Certyfikat ISO 9001, 14001, 50001 dla producenta sprzętu (należy dostarczyć na żądanie Zamawiającego).</p> <p>Deklaracja zgodności CE i ROHS (należy dostarczyć na żądanie Zamawiającego).</p> <p>Standard MIL-STD-810G (potwierdzony w oficjalnych dokumentach producenta lub załączonym wynikiem z przeprowadzonych testów)</p>
Oprogramowanie zabezpieczające – w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania	<p>System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej:</p> <ul style="list-style-type: none"> <li>wykrywanie i blokowanie plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,</li> <li>wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,</li> <li>wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)</li> </ul> <p>Szyfrowanie danych:</p> <ul style="list-style-type: none"> <li>Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.</li> <li>Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.</li> </ul> <p>Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.</p> <p>Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do</p>

stacji końcowej.

Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.

Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.

Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.

Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.

Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną anyransomware.

Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware.

Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:

- Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux
- Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.
- Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich
- Definiowanie struktury zarządzanie opartej o role i



polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji

Zarządzanie przez Chmurę:

1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach
2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury
3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur
4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy
5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach
6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń
7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej

Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.

Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.

1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer
2. Oprogramowanie klienckie, zarządzane z poziomu serwera.

System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:

- różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie
- funkcje przyznania praw dostępu dla nośników pamięci

tj. USB, CD

- funkcje regulowania połączeń WiFi i Bluetooth
- funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe
- funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi
- funkcje blokowania dostępu dowolnemu urządzeniu
- możliwość tymczasowego dodania dostępu do urządzenia przez administratora
- zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu
- możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka
- możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora
- możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich
- funkcję wirtualnej klawiatury
- możliwość blokowania każdej aplikacji
- możliwość zablokowania aplikacji w oparciu o kategorie
- możliwość dodania własnych aplikacji do listy zablokowanych
- zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsolę administracyjną na serwerze
- dodawanie innych aplikacji
- dodawanie aplikacji w formie portable
- możliwość wyboru pojedynczej aplikacji w konkretnej wersji
- dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB
- kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software,

#### encrypting tool

- możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.
- możliwość zablokowania funkcji Printscreen
- funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx
- funkcje monitorowania i kontroli przepływu poufnych informacji
- możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików
- możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj
- możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe
- ochronę przed wyciekami informacji na drukarki lokalne i sieciowe
- ochrona zawartości schowka systemu
- ochrona przed wyciekami informacji w poczcie e-mail w komunikacji SSL
- możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych
- ochrona plików zamkniętych w archiwach
- Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekami
- możliwość tworzenia profilu DLP dla każdej polityki
- wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania
- ochrona przed wyciekami plików poprzez programy typu p2p

#### Monitorowanie zmian w plikach:

- Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.

- Funkcje monitorowania określonych rodzajów plików.
- Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.
- Generator raportów do funkcjonalności monitora zmian w plikach.
- możliwość śledzenia zmian we wszystkich plikach
- możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach
- możliwość definiowania własnych typów plików

Optymalizacja systemu operacyjnego stacji klienckich:

- usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku
- optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem
- możliwość zaplanowania optymalizacji na wskazanych stacjach klienckich
- instruktaż stanowiskowy pracowników Zamawiającego
- dokumentacja techniczna w języku polskim

Oprogramowanie pozwalające na wykrywanie oraz zarządzaniu podatnościami bezpieczeństwa:

Wymagania dotyczące technologii:

1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową
2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.
3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:
  - Microsoft Internet Explorer
  - Microsoft Edge
  - Mozilla Firefox
  - Google Chrome

- Safari

4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących

5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie

6. Portal zarządzający musi umożliwiać:

a) przegląd wybranych danych na podstawie konfigurowalnych widgetów

b) zablokowania możliwości zmiany konfiguracji widgetów

c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.

d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności

e) eksport wszystkich skanów podatności do pliku CSV

Backup i przywracanie danych

- Deduplikacja danych,

- 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,



	<ul style="list-style-type: none"> <li>- Zapamiętywanie danych logowania,</li> <li>- Automatyczne uruchamianie programu przy starcie systemu,</li> <li>- Ustawianie priorytetu dla procesu backupu,</li> <li>- Zmiana klucza szyfrującego,</li> <li>- Ustawienia przepustowości/zajętości pasma,</li> <li>- Konfiguracja wydajności procesu backupu,</li> </ul> <p>Bezpieczeństwo</p> <ul style="list-style-type: none"> <li>- Zastępowanie nazwy pliku GUID-em,</li> <li>- Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,</li> <li>- Kompresja danych,</li> <li>- Transmisja po bezpiecznym protokole TLS,</li> <li>- Deklaracja klucza szyfrującego dane użytkownika,</li> <li>- Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,</li> <li>- Obliczanie sumy kontrolnej,</li> <li>- Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.</li> </ul> <p>WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze, Mac OS, Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji.</p>
<p>Wsparcie techniczne producenta</p>	<p>A) Dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta komputera numeru seryjnego lub modelu komputera – na wezwanie Zamawiającego należy dołączyć link strony.</p> <p>B) Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu</p>

Komputera.

C) W celu uniknięcia błędów kompatybilności Zamawiający wymaga, aby wszystkie elementy zestawu oraz podzespoły montowane przez Producenta były przez niego certyfikowane. Wykonawca niebędący producentem oferowanego sprzętu nie może samodzielnie dokonywać jego modyfikacji.