

DAI.261.14.2024

Załącznik nr 1 do SWZ

Opis przedmiotu zamówienia (OPZ)

I. CZĘŚĆ I – OPROGRAMOWANIE (LICENCJE) NR 1 – ODNOWIENIE LICENCJI I ZAKUP NOWYCH

- 1) **Pakiet oprogramowania biurowego do użytku offline wraz z wbudowanymi usługami chmurowymi 100% kompatybilny z używanym obecnie pakietem Microsoft 365 business standard (premium) o minimum 12 miesięcznym okresie ważności każdej z licencji.**

Wskazane poniżej, posiadane oprogramowanie, powinno być odnowione najpóźniej w chwili wygasania obecnie obowiązujących licencji, subskrypcji, wsparcia technicznego.

a) 71 szt. licencji zgodnych z przepisami RODO zawierające:

- edytor tekstu w wersji offline (możliwość instalacji w systemie Windows 10 i 11) oraz wersji chmurowej,
- arkusz kalkulacyjny w wersji offline (możliwość instalacji w systemie Windows 10 i 11) oraz w wersji chmurowej,
- program do przygotowania i prowadzenia prezentacji w wersji offline (możliwość instalacji w systemie Windows 10 i 11) oraz w wersji chmurowej,
- program do obsługi relacyjnych baz danych,
- system pocztowy do zarządzania pocztą elektroniczną, kalendarzem, kontaktami i zadaniami w wersji offline (możliwość instalacji w systemie Windows 10 i 11) oraz w wersji chmurowej. Usługa musi mieć możliwość konfiguracji skrzynek pocztowych o rozmiarze min. 50GB na użytkownika i wysyłania załączników o rozmiarze min. 70MB. System musi mieć możliwość pełnego nadzoru nad przesyłaną pocztą, oraz możliwość filtrowania przesyłanych treści (filtry antyspamowe)
- program do prowadzenia spotkań wideo oraz rozmów z wcześniej zaproszonymi użytkownikami w tej samej organizacji lub z osobami z poza organizacji w wersji offline (możliwość instalacji w systemie Windows 10 i 11) oraz w wersji chmurowej,
- przestrzeń dyskowa o pojemności min. 1TB w bezpiecznej konfigurowalnej chmurze do przechowywania plików lub udostępniania w i poza organizację,
- program do tworzenia publikacji;

Pakiet musi zawierać następujące funkcje i właściwości:

- cykliczne aktualizacje,
- wszystkie elementy pakietu muszą być integralną częścią tego pakietu i współpracować ze sobą,
- musi posiadać pomoc techniczną w ramach pakietu świadczoną w języku polskim (telefoniczna i chat),
- aplikacje offline oraz usługi chmurowe muszą posiadać polski interfejs (polska wersja językowa),
- możliwość współpracy na dokumentach (możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie – arkusz kalkulacyjny),
- możliwość tworzenia internetowych formularzy,
- posiadać pełną kompatybilność z systemami MS Windows 10 i 11 (32 i 64-bit),
- prawidłowe odczytywanie i zapisywanie danych w dokumentach w formacie: doc, docx, xls, xlsx, ppt, pptx, pps, ppsx,

- możliwość zapisu wytworzonych dokumentów w formacie PDF,
- możliwość planowania zadań dla użytkowników lub całych zespołów,
- możliwość tworzenia witryn internetowych (witryn zespołów),
- możliwość tworzenia automatyzacji pomiędzy aplikacjami pakietu,
- możliwość odnajdywania zawartości – wyszukiwanie,
- System musi posiadać wbudowane zabezpieczenia wraz z monitorowaniem,
- możliwość definiowania częstotliwości zmiany haseł przez użytkowników,
- możliwość używania 1 licencji oprogramowania na min. 3 niezależnych urządzeniach,
- możliwość integracji z MS Active Directory użytkowanym przez zamawiającego,
- dostępność usług na poziomie 99,9% czasu,
- dostępne wersje aplikacji na systemy android i iOS (poczta, zarządzanie plikami);

Czas rozpoczęcia ważności dostarczonych licencji – od 01.12.2024 r.

Zamawiający zezwala aby licencje - numery do aktywacji, były dostarczone w formie fizycznej - o ile są dostępne, umożliwiające zamawiającemu odnowienie licencji już posiadanej lub zarejestrowanie licencji jako kolejnej - nowej.

b) 8 szt. licencji zgodnych z przepisami RODO zawierające właściwości pakietu z pkt. a) oraz dodatkowo:

- możliwość zarządzania urządzeniami mobilnymi i aplikacjami
- zaawansowana ochrona przed zagrożeniami
- zdalne wymazywanie urządzeń

Czas rozpoczęcia ważności dostarczonych licencji – od 01.12.2024 r.

Zamawiający zezwala aby licencje - numery do aktywacji, były dostarczone w formie fizycznej - o ile są dostępne, umożliwiające zamawiającemu odnowienie licencji już posiadanej lub zarejestrowanie licencji jako kolejnej - nowej.

2) Veeam Backup Essentials Universal Perpetual Enterprise Plus – 4 szt. (20 instancji) – odnowienie wsparcia na 3 lata

Oprogramowanie w wersji (perpetual) – licencje odnowienia wsparcia na 3 lata dla 20 instancji.

3) Licencje CAL dla Windows Serwer 2022 (2025) – 35 szt. (na użytkownika) oraz 35 szt. (na urządzenie)

4) Licencje CAL dla MS SQL Serwer 2019 - 15 szt. (na użytkownika)

II. CZĘŚĆ II – OPROGRAMOWANIE ANTYWIRUSOWE Z XDR Z WDROŻENIEM (LICENCJE) NR 2

- 1) Oprogramowanie antywirusowe wraz z wymienionymi funkcjonalnościami bezpieczeństwa wraz z usługą wdrożenia dla:
- 90 stacji roboczych
 - 10 serwerów Windows
 - 5 serwerów linux
 - 20 urządzeń mobilnych (posiadane systemy - Android, IOS)

Usługa wdrożenia musi zostać zrealizowana do **15.12.2024**

Opis wymaganych funkcjonalności:**a) Administracja zdalna w chmurze**

- Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
- Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
- Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
- Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
- Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
- Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
- Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
- Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
- Rozwiązanie musi posiadać kilkadziesiąt szablonów raportów, przygotowanych przez producenta.
- Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
- Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
- Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

b) Ochrona stacji roboczych

- Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
- Rozwiązanie musi wspierać architekturę ARM64.
- Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
- Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
- Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
- Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
- Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
- Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
- Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
- Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
- Rozwiązanie musi posiadać wbudowane moduły heurystyczne.

- Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
- Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
- Moduł HIPS (system zapobiegania włamaniom) musi posiadać możliwość pracy w trybach : tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
- Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
- Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
- Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
- Rozwiązanie musi być wyposażone w moduł bezpiecznej przeglądarki.
- Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
- Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
- Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
- Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o zdefiniowane kategorie i podkategorie.
- Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
- W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

c) Ochrona serwera

- Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
- Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
- Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
- Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

- Rozwiązanie musi posiadać wbudowane moduły heurystyczne
- Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
- Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

- Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
- Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
- Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
- Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
- Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
- Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikację, czynność oraz adres IP.
- Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup

Dodatkowe wymagania dla ochrony serwerów Linux:

- Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
- Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
- Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonych mikro-serwisu.

d) Szyfrowanie

- System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
- Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
- Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI.

e) Ochrona urządzeń mobilnych opartych o system Android

- Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
- Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
- Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
- Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: usunięcie zawartości urządzenia, przywrócenie urządzenia do ustawień fabrycznych, zablokowania urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS.
- Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.

- Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła.

f) Ochrona serwera pocztowego MS Exchange (Exchange online oraz Microsoft 365 w tym aplikacji)

- Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.
- Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.
- Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
- Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
- Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
- Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
- Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
- System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
- Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
- Rozwiązanie ma posiadać mechanizm greylisting (szara lista).
- Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

g) Sandbox w chmurze

- Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
- Rozwiązanie musi wykorzystywać do działania chmurę producenta.
- Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
- Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
- Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
- Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
- Po zakończonej analizie pliku, rozwiązanie musi przysyłać wynik analizy do wszystkich wspieranych produktów.
- Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
- Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
- Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
- Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzewać jakie pliki zostały wysłane do analizy oraz przez kogo.
- Przeanalizowane pliki muszą zostać odpowiednio oznaczone.
- W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
- W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbek.

- Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

h) Ochrona usługi Microsoft 365

- Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.
- Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Microsoft 365.
- Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
- Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
- Rozwiązanie musi być dostępny w języku polskim.
- Konsola rozwiązania musi posiadać możliwość raportowania co najmniej: użytkowników, otrzymujących najwięcej spamu, użytkowników, otrzymujących najwięcej wiadomości typu „phishing”, użytkowników, otrzymujących największą ilość szkodliwego oprogramowania, kont użytkowników, które mogą być podejrzane.
- Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.
- Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej: jaka ilość wiadomości została przeskanowana, wynik skanowania poszczególnych wiadomości, czynność podjęta przez rozwiązanie.
- Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o: zagrożeniach, które zostały wykryte, na jakim koncie zostały wykryte, jakie zagrożenie zostało wykryte, podjętą czynność.
- Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
- Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
- Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
- Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:
 - wykorzystania do analizy mechanizmów chmurowych, tego samego producenta, wprowadzenia białych i czarnych list adresów ochrony Exchange’a Online, dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
- Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
- Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
- Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
- Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
- Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

i) Moduł XDR

- Dostęp do konsoli centralnego zarządzania może odbywać się z poziomu interfejsu WWW.
- Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
- Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
- Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

- Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
- Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
- Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
- Serwer musi posiadać wbudowane reguły, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
- Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
- Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
- Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
- Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
- W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
- W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
- Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
- Konsola administracyjna musi mieć możliwość tagowania obiektów.
- Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

j) Moduł podwójnej autentykacji (uwierzelnianie wieloskładnikowe)

- Uwierzelnianie wieloskładnikowe powinno być możliwe do wykorzystania w logowaniu VPN (Fortinet), logowaniu domenowym lub logowaniu do aplikacji

Dodatkowe wymagania

- Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.
- Rozwiązanie musi wspierać system operacyjny Windows 10 / Windows 11.
- Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
- Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019.
- Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 / 2019.

- Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access.
- Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Access.
- Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access.
- Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
- Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).
- Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.
- Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
- Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
- Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.
- Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego

Wymagania Ogólne:

- **Wykonawca zamówienia musi świadczyć wsparcie techniczne do zaoferowanego systemu także w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu.**
- **Wykonawca wdroży oprogramowanie zg. z wymaganiami zamawiającego i jego bieżącymi potrzebami.**

III. CZĘŚĆ III – OPROGRAMOWANIE (LICENCJE) NR 3 – ODNOWIENIE LICENCJI I ZAKUP NOWYCH**1) Odnowienie licencji (zakup nowych) - wsparcia technicznego – Axence Nvision na okres 1 roku**

Przedłużenie ważności umowy serwisowej dla 85 urządzeń i dokupienie 5 szt. licencji (łącznie 90 szt.) dla modułów:

- Network,
- Helpdesk,
- DataGuard
- Inventory (dokupienie modułu)

2) Platforma szkoleniowa do spraw cyberbezpieczeństwa i Rodo dla 85 użytkowników.

- Platforma musi oferować samodzielny cykl szkoleń dla każdego użytkownika w celu realizowania szkoleń cyklicznych w ww. tematach.
- Platforma musi zawierać lekcje, testy i zadania które pomogą zrozumieć problematykę cyberbezpieczeństwa.
- Platforma ma pozwalać na monitorowanie postępów w nauce

IV. CZĘŚĆ IV. – OPROGRAMOWANIE (LICENCJE) NR 4 - ODNOWIENIE LICENCJI NA OPROGRAMOWANIE LOG360 I VULNERABILITY MANAGER PLUS wraz ze wsparciem technicznym w języku polskim.**1) Odnowienie/dokupienie brakujących licencji na okres 1 roku dla LOG 360 na:**

- 25 urządzeń,

- 5 Aplikacji,
- 90 Stacji Roboczych,
- 10 Windows Serwerów,
- 3 Serwerów IIS,
- 2 Serwera SQL,
- 2 Serwerów Plików Linux,
- 2 Kontrolerów domeny,
- 2 Serwerów Plików Windows,
- 1 Serwer NAS.

- 2) Odnowienie/dokupienie brakujących licencji na okres 1 roku dla VULNERABILITY MANAGER PLUS (Enterprise Edition) na **15 serwerów i 90 stacji roboczych**.

V. CZĘŚĆ V. – SPRZĘT KOMPUTEROWY Z OPROGRAMOWANIEM (laptopy, monitory, peryferia)

- 1) Komputery przenośne wraz z dodatkowym wyposażeniem – 15 szt.

Lp.	Opis elementów	Wymagania minimalne
1.	Typ	Komputer przenośny - laptop
2.	Parametry techniczne	<p>Procesor</p> <ul style="list-style-type: none"> - osiągający wynik min.17000[pkt.] w benchmark passmark (cpu mark) <p>Urządzenie musi być wyposażone w technologię zdalnego dostępu do zasobów (bios, system operacyjny) w celu zdalnego zarządzania.</p> <p>Ekran</p> <ul style="list-style-type: none"> - Wielkość matrycy [cale] 15,6 – max. 16 - Rodzaj matrycy fhd [led] ips 250n - Rozdzielczość (pixele) 1920 x 1080 - Technologia matrycy matowa (anti-glare) <p>Dysk twardy</p> <ul style="list-style-type: none"> - Pojemność: 512 gb - Typ ssd m.2 nvme <p>Pamięć ram</p> <ul style="list-style-type: none"> - 16 GB - Ilość banków pamięci min. 2 - Max. wielkość pamięci min.32 GB - Taktowanie [mhz] min. 5200 <p>Karta graficzna</p> <ul style="list-style-type: none"> - Zintegrowana lub dedykowana min. HD tj.1920x1080

		<p>Złącza</p> <ul style="list-style-type: none"> - Gniazdo słuchawkowe, - Mikrofon/słuchawki - USB 3.2 Gen. 1 lub 2 - Usb-C gen 1 lub 2 - Rj-45 (ethernet) Gb/s lub karta zewnętrzna jako przejściówka USB - Czytnik kart pamięci <p>Multimedia</p> <ul style="list-style-type: none"> - Karta dźwiękowa - Głośniki wbudowane stereo - Mikrofon - Kamera internetowa min.720p <p>Komunikacja</p> <ul style="list-style-type: none"> - Karta sieciowa lan [mbps] 1000 Rj-45 (ethernet) - Karta bezprzewodowa wifi - 11ax - Bluetooth <p>Klawiatura/wskaźniki</p> <ul style="list-style-type: none"> - Klawiatura podświetlana <p>Bezpieczeństwo</p> <ul style="list-style-type: none"> - Czytnik linii papilarnych - Szyfrowanie TPM - Gniazdo blokady bezpieczeństwa - Szyfrowanie dysku - Bateria (czas pracy) min. 5 godz. - Zainstalowany system operacyjny w polskiej wersji językowej: <p>Kompatybilny i obsługujący Active Directory</p> <p>Wykorzystujący najnowsze standardy bezpieczeństwa</p> <ul style="list-style-type: none"> - DODATKOWO POWINIEN POSIADAĆ: <ul style="list-style-type: none"> • Firewall systemowy • Przywracanie systemu • Wbudowane oprogramowanie chroniące przed programami szpiegującymi • kompatybilność z najnowszym oprogramowaniem biurowym Office 365 wykorzystywanym w funduszu • Wyszukiwarka plików • Obsługa pulpitu zdalnego
--	--	--

		<ul style="list-style-type: none"> • Zoptymalizowana obsługa komputerów typu tablet • Kopia zapasowa w tle • Interfejs w języku polskim • System 64 bitowy • Funkcjonalność oferująca łatwy transfer plików na nowy system operacyjny • Rozpoznawanie bieżącej lokacji użytkownika na potrzeby drukowania dokumentów • Wbudowany wirtualizator • Pozwalać na konfiguracje poprzez MS Active Directory GPO
3.	Certyfikaty	Certyfikat CE
4.	Gwarancja	<ul style="list-style-type: none"> - min. 36 m-cy - Usługi gwarancyjne świadczone na miejscu - Sprzęt musi pochodzić z polskiej dystrybucji - W przypadku uszkodzenia dysku dysk pozostaje u zamawiającego
5.	Dodatkowe wyposażenie	<ul style="list-style-type: none"> • 10 szt. stacja dokująca wyposażona w : <ul style="list-style-type: none"> - niezależne zasilanie (odrębny zasilacz) Złącza: <ul style="list-style-type: none"> - 3 x USB 3.1, - USB typu C, - HDMI, - DisplayPort, - RJ-45 Gigabit Ethernet - gniazdo słuchawkowe - przycisk zasilania - Gwarancja min. 12 m-cy • 20 szt. torba na komputer przenośny: <ul style="list-style-type: none"> - Na komputer o wymiarach 15,6", - min. 2 kieszenie zasuwane na zamek błyskawiczny, - materiał przeważający poliester, - kolor ciemny, - wodoodporna, - wyposażona w rączkę wzmacnianą i pasek na ramie, - Gwarancja min. 12 m-cy • 25 szt. zestawów bezprzewodowych klawiatura + mysz: <ul style="list-style-type: none"> - klawiatura koloru czarnego, - szyfrowanie komunikacji bezprzewodowej, - odporne na ścieranie nadruki klawiszy, - polski układ klawiszy , - klawiatura z klawiaturą numeryczną, - regulacja min. 2 pozycji nachylenia klawiatury,

		<ul style="list-style-type: none"> - zasięg bezprzewodowy min. 10 m., - odbiornik sygnału USB, - posiadająca wyłącznik, - dodatkowe przyciski funkcyjne - wskaźnik Caps Lock, - wskaźnik baterii, - wyprofilowana mysz pasująca do obu dłoni, - mysz wyposażona w min. 2 przyciski, - mysz wyposażona w wyłącznik, - zestaw wyposażony w baterie AAA lub AA (max. 3 szt), - min. 24 m-ce gwarancji; <ul style="list-style-type: none"> • 60 szt. - podkładki pod mysz (żelowe) <ul style="list-style-type: none"> - żelowa podkładka pod nadgarstek i mysz - wykonane z materiału łatwego do czyszczenia-dezynfekcji (nie materiałowe) min. 12 m-cy gwarancji; • Patchcordy 6 kat. <ul style="list-style-type: none"> - 10 szt. – 10 m - 10 szt. – 5 m - 10 szt. – 1 m - 10 szt. – 0.5 m • 5 szt. Listwa zasilająca antyprzepięciowa - długość przewodu 3 m. • 5 szt. Listwa zasilająca antyprzepięciowa - długość przewodu 5 m. • 20 szt. słuchawek przewodowych z mikrofonem USB <ul style="list-style-type: none"> - Konstrukcja słuchawek - Nauszne - Gwarancja producenta -3 lata - Przeznaczenie - Telefonii internetowa - Złącza - 1 x USB 2.0 - Dźwięk (słuchawki) - Stereo - Kontrola dźwięku - Regulacja głośności, Odbieranie/Wyciszanie połączenia - Mikrofon - Na pałku - Redukcja szumów - Kolor - ciemny lub Czarny • 30 szt. zasilaczy do już posiadanych stacji dokujących i-tec – 100W – USB-C PD
--	--	---

2) 10 szt. monitorów komputerowych 24",

Lp.	Opis elementów	Wymagania minimalne
1.	Typ	Monitor komputerowy
2.	Parametry techniczne	<ul style="list-style-type: none"> - przekątna ekranu min. 23,8 cali, max. 24 cali - typ ekranu IPS, - wejścia wideo: hdmi, displayport, - matowa matryca (anty-glare), - rozdzielczość ekranu min. 1920x1080, - czas reakcji matrycy max. 5 ms, - jasność min. 250 cd/m2, - kontrast min.1000:1, - kąt widzenia pionowy i poziomy min. 170, - wbudowane głośniki - wbudowany mikrofon, - wbudowana kamera, - możliwość pochylenia monitora, - kpl. przewodów: zasilania, sygnałowy displayport, hdmi, - kolor szary (srebrny) lub czarny
3.	Certyfikaty	<ul style="list-style-type: none"> - Certyfikat CE - EnergyStar
4.	Gwarancja	<ul style="list-style-type: none"> - gwarancja min. 36 m-cy - Sprzęt musi pochodzić z polskiej dystrybucji

3) 20 szt. monitorów komputerowych 27",

Lp.	Opis elementów	Wymagania minimalne
1.	Typ	Monitor komputerowy
2.	Parametry techniczne	<ul style="list-style-type: none"> - przekątna ekranu min. 27 cali, max. 27 cali - typ ekranu IPS, - wejścia wideo: hdmi, displayport, usb-c - matowa matryca (anty-glare), - rozdzielczość ekranu min. 1920x1080, - czas reakcji matrycy max. 8 ms, - jasność min. 300 cd/m2, - kontrast min.1000:1, - kąt widzenia pionowy i poziomy min. 170, - wbudowane głośniki - wbudowany mikrofon, - wbudowana kamera, - wbudowany hub usb-c, - wbudowana karta sieciowa RJ45 - możliwość pochylenia monitora, - kpl. przewodów: zasilania, sygnałowy displayport, hdmi, usb-c - kolor szary (srebrny) lub czarny
3.	Certyfikaty	<ul style="list-style-type: none"> - Certyfikat CE - EnergyStar

4.	Gwarancja	<ul style="list-style-type: none"> - gwarancja min. 36 m-cy - Sprzęt musi pochodzić z polskiej dystrybucji
----	-----------	--

VI. CZĘŚĆ VI. – Urządzenie wielofunkcyjne kolorowe A3/A4 (kserokopiarka) z usługą wstępnej instalacji i konfiguracji – 1 szt.

Lp.	Opis elementów	Wymagania minimalne
1.	Typ	Kserokopiarka kolorowa A3/A4
2.	Parametry techniczne	<ul style="list-style-type: none"> - Szybkość urządzenia, tryb cz.-b. w str./min(A4) - 31 - Szybkość urządzenia, tryb kolorowy w str./min (A3) - 15 - Szybkość urządzenia, tryb cz.-b. w str./min (A3) - 15 - Format papieru: min.- maks. A6R - SRA3 - Gramatura papieru (g/m²) 55 - 300 - Pojemność: standardowa (arkuszy) 650 - Pojemność: maks. (arkuszy) 6300 - Czas nagrzewania (w sekundach) 18 - Pojemność SSD (GB) 256 - Dupleks - Wymagania dotyczące źródła zasilania - 200–240 V, 50 / 60 Hz - Pojemność dodatkowego podajnika oryginałów (kartek) 200 - Wyświetlacz kolorowy min. 9 cali <p>FUNKCJE ARCHIWIZACJI DOKUMENTÓW</p> <ul style="list-style-type: none"> - Funkcja archiwizacji dokumentów - Pojemność funkcji przechowywania dokumentów - foldery główny i własny (liczba stron) - 20000 - Pojemność funkcji przechowywania dokumentów - folder tymczasowy (liczba stron) - 10000 - Programowane zadania: Kopiowanie, drukowanie, skanowanie - Foldery do przechowywania dokumentów Folder tymczasowy, folder główny, - foldery własne (maks. 1000) <p>SIEĆ BEZPRZEWODOWA</p> <ul style="list-style-type: none"> - Zgodność IEEE802.11 a / b / g / n / ac - Bezpieczeństwo WEP, WPA / WPA2-mieszany PSK, WPA / WPA2-mieszany EAP, WPA2-PSK, WPA2-EAP, WPA2 / WPA3-mieszany PSK / SAE, WPA3 SAE, WPA2 / WPA3-mieszany EAP, WPA3 EAP <p>KOPIARKA</p> <ul style="list-style-type: none"> - Format oryginału (maks.) A3

		<ul style="list-style-type: none"> - Czas pierwszej kopii kolorowej (sek.) 8 - Czas pierwszej kopii cz.-b. (sek.) 6 - Sorter elektroniczny - Kopiowanie ciągłe (maks. kopii) 9,999 - Rozdzielczość skanowania w trybie cz.-b. (dpi) 600 x 600, 600 x 400 - Rozdzielczość skanowania w trybie kolorowym (dpi) 600 x 600 - Rozdzielczość druku (dpi) 1200 x 1200, 600 x 600, 9600 x 600 - Gradacja (liczba odcieni) - tryb kolorowy 256 - Zakres regulacji skali (%) 25 – 400 <p>SKANER</p> <ul style="list-style-type: none"> - Skaner sieciowy: - Skanowanie na pulpit - Skanowanie do FTP, Email - Skanowanie do folderu sieciowego - Skanowanie do pamięci USB - Formaty plików TIFF, PDF, PDF / A-1a, PDF / A-1b, szyfrowany PDF, kompaktowy PDF, JPEG, XPS, przeszukiwalny PDF, Microsoft Office (pptx, xlsx, docx), TXT (UTF-8), RTF - Jednoprzebiegowy - Skanowanie do 280 obrazów/min. <p>DRUKARKA</p> <ul style="list-style-type: none"> - Rozdzielczość (dpi) 1200 x 1200, 600 x 600, 9600 x 600 - Drukarka sieciowa (std./opcja) Ethernet w standardzie - Interfejs standardowy/opcjonalny USB 2.0, USB 3.0, 10Base-T / 100Base-TX / 1000Base-T, - opcjonalnie obsługa drugiej sieci LAN - Obsługiwane systemy operacyjne – Windows 10, 11, Windows Server 2012, 2012R2, 2016, 2019. - Mac OS X 10.10, 10.11, 10.12, 10.13, 10.14, 10.15, 11, 12 - Protokoły sieciowe TCP / IP (IPv4, IPv6) - Protokoły druku LPR, Raw TCP (port 9100), POP3 (drukowanie przez e-mail), HTTP, - FTP do pobierania plików do druku, IPP, SMB, WSD - W standardzie emulacja PCL 6, - Obsługa Adobe® PostScript® 3™ <p>OPCJE WYKOŃCZENIA (możliwe do zainstalowania- nie wymagane obecnie)</p>
--	--	---

		<ul style="list-style-type: none"> - Zszywanie broszur - Dziurkacz <p>OPCJE WYKOŃCZENIA</p> <ul style="list-style-type: none"> - Przesunięcie offsetowe -wymagane <p>WYDAJNOŚĆ TONERA</p> <ul style="list-style-type: none"> - Czarny (stron przy 5% pokryciu) 30000 - Cyan (stron przy 5% pokryciu) 20000 - Magenta (stron przy 5% pokryciu) 20000 - Żółty (stron przy 5% pokryciu) 20000 <p>WYPOSAŻENIE DODATKOWE</p> <ul style="list-style-type: none"> - Podstawa z kasetami min. 2 kasety dla A3 lub A4 dla min. 1000 arkuszy (łącznie)
3.	Dodatkowe funkcje wymagane	<ul style="list-style-type: none"> - integracja i połączenie z aplikacjami procesów biznesowych w chmurze - Wbudowane złącze Microsoft Teams usprawnia współpracę, zapewniając bezpośredni i bezpieczny dostęp do drukowania lub skanowania z kanałów Microsoft Teams - funkcje ochrony systemu i danych, w tym zabezpieczenia oparte na systemie BIOS, standardowy moduł TPM (Trusted Platform Module) zapewniają bezpieczeństwo poufnych danych - Interakcja z urządzeniem wielofunkcyjnym bezpośrednio z urządzenia mobilnego poprzez Wi-Fi, AirPrint, Bluetooth, NFC i kod QR - Obsługa czytnika kart (standard Unique 125kHz) – karty wykorzystywane też do RCP - Wydruk nadzorowany po kodzie użytkownika i loginie i hasle domenowym (LDAP)
4.	Dodatkowe wymagania	<ul style="list-style-type: none"> - Dostawa 3 kpl. tonerów wraz z urządzeniem (CMYK) - Pojemnik na zużyty toner - Instalacja i wstępna konfiguracja sprzętu wraz ze wstępnym przeszkoleniem
5.	Gwarancja	<ul style="list-style-type: none"> - min. 24 m-ce

VII. CZĘŚĆ VII. – Urządzenia dostępne Access Point – 5 szt. (zarządzalne) z wdrożeniem oraz wsparcie techniczne dla posiadanych przełączników Alcatel.
1) Urządzenia dostępne Access Point – 5 szt. (zarządzalne) z wdrożeniem

Lp.	Opis elementów	Wymagania minimalne
1.	Typ	Access Point WIFI
2.	Parametry techniczne	<ul style="list-style-type: none"> - Urządzenie musi być kompatybilne z systemem OmniVista 2500 i możliwe do konfiguracji za jego pomocą - Wewnętrzne urządzenie dostępne - Musi posiadać wewnętrzne anteny zintegrowane w obudowie - Urządzenie musi obsługiwać standard 802.11ax i WIFI 6 i być wstecznie kompatybilne - Przepustowość 3Gbps - Praca w pasmach Wi-Fi 2,4 GHz i 5 GHz - Wielodostęp z podziałem częstotliwości (OFDMA), - wiele wejść dla wielu użytkowników, wiele wyjść (MU-MIMO), - tryb kwadraturowej modulacji amplitudy 1024 (1024-QAM), - budzenie docelowe czas (TWT) i nadawanie kształtowania wiązki. - Obsługuje precyzyjnie dostrojone parametry jakości usług (QoS) w celu rozróżnienia i zapewnienia odpowiedniego QoS dla każdej aplikacji, takiej jak głos, wideo i udostępnianie pulpitu - Możliwość logicznego grupowania punktów dostępowych - Możliwość pracy w architekturze klastra AP - Obsługa Bluetooth - Sygnalizacja świetlna stanu urządzenia - Wbudowany Zintegrowany moduł Trusted Platform Module - Obsługa WPA2, WPA3, AES, TKIP - Obsługa zapory: ACL, IPS, IDS i współpraca zasad aplikacji z systemem OmniVista - Obsługa zasilania POE - Możliwość zasilania przez zewnętrzne źródło prądu - Obsługa do 1000 urządzeń klienckich - Obsługa do 30 SSID - Automatyczny wybór kanału - Automatyczna kontrola mocy transmisji - Kontrola przepustowości na SSID - Roaming L2 i Roaming L3 - Portal uwierzytelniający (wewnętrzny/zewnętrzny) - Samodzielna rejestracja gościa (opcjonalne powiadomienie SMS) - Wewnętrzna baza danych użytkowników - Klient RADIUS - Uwierzytelnianie proxy RADIUS

		<ul style="list-style-type: none"> - Uwierzytelnianie proxy LDAP/AD - równoważenie obciążenia klienta - Śledzenie zachowań użytkowników - Biała/czarna lista - Zero-touch provisioning (ZTP) - Klient NTP - DHCP/DNS/NAT - Bezprzewodowa sieć MESH P2P/P2MP - Lokalizacja i ograniczenie nieuczciwych punktów dostępowych - Raport dziennika systemowego SSHv2, SNMPv2, SNMPv3 - Wykrywanie ataków bezprzewodowych - Plan piętra z wizualizacją mapy cieplnej <p>INTERFEJSY</p> <ul style="list-style-type: none"> - 10BASE-T/100BASE-TX/1000BASE-T/2500BASE-T IEEE 802.3 - (RJ-45) port, ENET0, Power over Ethernet (PoE) 802.3at compliant, 802.3az - Ethernet (EEE) - 10/100/1000 BASE-T IEEE 802.3 compliant auto-sensing (RJ-45), Power over Ethernet - (PoE) 802.3at compliant, 802.3az Energy Efficient Ethernet (EEE) - USB 2.0 Type A - Factory reset <p>STANDARD IEEE</p> <ul style="list-style-type: none"> - IEEE 802.11a/b/g/n/ac/ax - IEEE 802.11e WMM, U-APSD - IEEE 802.11h, 802.11i, - 802.11e QoS - IEEE 802.1Q (tagowanie VLAN) - Zarządzanie zasobami radiowymi 802.11k - Zarządzanie przejściem BSS 802.11v - Szybki roaming 802.11r - Chroniona ramka zarządzania 802.11w
3	Wyposażenie	Elementy pozwalające zwiesić urządzenie na ścianie
4.	Gwarancja	<ul style="list-style-type: none"> - Gwarancja do końca wsparcia producenta (min. 36 m-cy) - Wsparcie techniczne min. 1 rok (wykonawca zamówienia musi móc świadczyć wsparcie techniczne dla zaoferowanych urządzeń)

2) Odnowienie wsparcia technicznego dla 4 przełączników Alcatel OS6560-48X4 – na okres 12 m-cy