

GK.041.1.2024

OPIS PRZEDMIOTU ZAMÓWIENIA

**„Podniesienie stopnia bezpieczeństwa IT w urzędzie gminy Chrostkowo w ramach projektu
Cyberbezpieczny Samorząd”**

Zamawiający:

Chrostkowo

DOSTAWA INFRASTRUKTURY SPRZĘTOWEJ ORAZ OPROGRAMOWANIA

Przedmiotem zamówienia jest dostawa sprzętu i oprogramowania podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych w urzędzie gminy Chrostkowo.

Poniżej wyspecyfikowano minimalne parametry sprzętu oraz oprogramowania, które należy dostarczyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

Wymagania ogólne:

- Całość dostarczanego sprzętu i oprogramowania standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
- Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, musi być nowe, wcześniej nieużywane, rok produkcji nie starszy niż 2023.
- Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, w którym nie wskazano szczegółowych warunków gwarancji, musi być objęte minimum 24 miesięczną gwarancją jeśli w opisie parametrów nie wskazano inaczej
- Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
- Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
- Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
- Wszystkie urządzenia muszą posiadać oznakowanie CE.
- Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
- Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V \pm 10%, 50 Hz.
- Wymagane jest, aby infrastruktura sprzętowa była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
- Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).

Zamawiający wymaga aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:

- posiadane środowisko domenowe,
- posiadaną konfigurację sieci wraz z segmentacją VLAN, oraz strefą DMZ,
- posiadaną konfiguracją baz danych i backupów,
- konfigurację stacji roboczych.

Wykonawca w ramach postępowania zobowiązany jest do wykonania co najmniej następujących usług związanych z montażem i konfiguracją dostarczanej infrastruktury sprzętowej:

1. Wykonanie Projektu Technicznego dostarczanej infrastruktury sprzętowej, który będzie składał się co najmniej z następujących elementów:

- Dokładna specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów,
- Nazwy oraz szczegółowa adresacja poszczególnych elementów,
- Planowana konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsca, zaprojektowanie kompleksowego systemu ochrony danych opartego na funkcjach macierzy oraz oprogramowania standardowego z uwzględnieniem specyfiki całego projektu,
- Wymagane działania ze strony Zamawiającego w celu poprawnego montażu i konfiguracji,
- Harmonogram prac.

Projekt techniczny musi zostać wykonany po wcześniejszej analizie środowiska wykonanej przez Wykonawcę oraz musi zostać zaakceptowany przez Zamawiającego.

2. Konfiguracja serwerów oraz macierzy dyskowej.
3. Instalacja oraz konfiguracji oprogramowania.
4. Testy rozwiązania.
5. Instruktaż dla administratorów demonstrujący sposób zarządzania środowiskiem.
6. Dostarczenie dokumentacji powykonawczej infrastruktury sprzętowej i oprogramowania standardowego, która będzie składała się co najmniej z następujących elementów:
 - Specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów oraz numerami seryjnymi poszczególnych elementów,
 - Końcowe nazwy oraz szczegółowa adresacja poszczególnych elementów,
 - Konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsc
 - Komplet poświadczeń do całej infrastruktury – wymagana zmiana haseł domyślnych – dostarczone jako osobny załącznik w postaci zaszyfrowanego pliku kdbx,
 - Dokumentacja techniczna w formie elektronicznej do każdego elementu w języku polskim lub angielskim
 - Szczegóły dotyczące instalacji i uruchomienia infrastruktury sprzętowej, w zakresie modernizacji infrastruktury szpitala, zostaną ustalone pomiędzy Stronami w trakcie Analizy Przedwdrożeniowej.
 - Zamawiający zapewni odpowiedni zapas mocy oraz odpowiednie warunki środowiskowe w komorach serwerowni.
 - Po zakończonym montażu Wykonawca przekaze Zamawiającemu wszystkie hasła dostępne do kont „super użytkowników”.

Opis parametrów minimalnych dostarczanej infrastruktury oraz oprogramowania:

Wymagania dla Wykonawcy który dostarczy infrastrukturę sprzętową oraz oprogramowanie:

Zamawiający wymaga, aby Wykonawca spełniała wymagania w zakresie:

Zestawienie wymaganego sprzętu i oprogramowania

Lp.	Typ sprzętu	Ilość
1.	Oprogramowanie EDR plus serwer	1 klp.
2.	Oprogramowanie do Inwentaryzacji aktywów i ich konfiguracji	1 klp.
3.	NAS Klasy Enterprise	1 szt.
4.	NAS	1 szt.
5.	Szkolenie dla pracowników IT	1 klp.

1. Oprogramowanie EDR plus serwer

Nazwa producenta:

Nazwa i typ:

System EDR – do 35 stanowisk			
Lp.	Wymagane minimalne parametry techniczne	Wymóg do spełnienia (warunek graniczny)	OFEROWANE PARAMETRY TECHNICZNE - podaje Wykonawca <u>Wymogi dotyczące opisu oferowanych parametrów:</u> TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę NIE – wykonawca nie spełnia konkretnego parametru
Ochrona stacji roboczych - Windows			
1.	<ul style="list-style-type: none"> Rozwiązanie musi wspierać systemy operacyjne Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows. Rozwiązanie musi wspierać architekturę ARM64. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim. Skuteczność rozwiązania potwierdzona nagrodami VB100 i AV-comparatives. 	TAK	
Ochrona antywirusowa i antyspyware			
1.	<ul style="list-style-type: none"> Rozwiązanie musi zapewniać pełną 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 posiadać wbudowaną technologię do ochrony przed rootkitami. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu. Rozwiązanie musi posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem 	TAK	

<p>sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.</p> <ul style="list-style-type: none"> ▪ Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). ▪ Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. ▪ Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. ▪ Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych. ▪ Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. ▪ Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. ▪ Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku. ▪ Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. ▪ Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. ▪ Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera. ▪ W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. ▪ Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. ▪ Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. ▪ Rozwiązanie musi posiadać wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. ▪ Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. ▪ Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), 		
--	--	--

<p>zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).</p> <ul style="list-style-type: none"> ▪ Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. ▪ Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. ▪ Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie. ▪ Rozwiązanie musi posiadać możliwość blokowania możliwości przeglądania wybranych stron internetowych. Rozwiązanie musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL. ▪ Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora. ▪ Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. ▪ Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. ▪ Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe. ▪ Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta. ▪ Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego. ▪ Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. ▪ Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym. ▪ Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. ▪ W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne. ▪ Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość 		
---	--	--

<p>wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p> <ul style="list-style-type: none"> ▪ Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie. ▪ Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika. ▪ Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. ▪ Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. ▪ Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. ▪ Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło. ▪ Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo. ▪ Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji. ▪ Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. ▪ Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń. ▪ System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. ▪ System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. ▪ Rozwiązanie musi posiadać umożliwiać administratorowi 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. 		
---	--	--

<ul style="list-style-type: none"> ▪ Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia. ▪ Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. ▪ Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia. ▪ Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. ▪ W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. ▪ Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika. ▪ Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS). ▪ Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: <ul style="list-style-type: none"> • 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. ▪ Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. ▪ Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. ▪ Rozwiązanie musi posiadać zaawansowany skaner pamięci. ▪ Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej 		
--	--	--

	<p>czynnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.</p> <ul style="list-style-type: none"> 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. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. Rozwiązanie musi posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antyvirus, antyspyware, metody heurystyczne). Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym. W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym. Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń. Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z 		
--	---	--	--

<p>poziomu interfejsu aplikacji.</p> <ul style="list-style-type: none"> ▪ Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline. ▪ Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie. ▪ W trakcie instalacji rozwiązanie ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM. ▪ W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji. ▪ Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej. ▪ Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia. ▪ Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny. ▪ Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. ▪ Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki. ▪ Rozwiązanie musi posiadać możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych. ▪ Rozwiązanie musi posiadać możliwość definiowania stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji. ▪ Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie. ▪ Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. ▪ Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia. ▪ Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup. ▪ Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny. ▪ Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”. 		
--	--	--

	<ul style="list-style-type: none"> Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet. Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB. Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu. 		
Ochrona przed spamem			
1.	<ul style="list-style-type: none"> Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. Rozwiązanie musi umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. Rozwiązanie musi umożliwiać automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. Rozwiązanie musi posiadać możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego. Rozwiązanie musi posiadać możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego. Rozwiązanie musi posiadać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam. Rozwiązanie musi umożliwiać zdefiniowanie dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam. Rozwiązanie musi domyślnie współpracować z folderem „Wiadomości-śmieci”, dostępnym w programie Microsoft Outlook. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana” Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądaną na spam oznaczy ją jako „przeczytana”. Rozwiązanie musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera. 	TAK	

Zapora osobista (personal firewall)

1.	<ul style="list-style-type: none"> ▪ Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: <ul style="list-style-type: none"> – 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 oceniać reguły zapory systemu Windows. ▪ Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych. ▪ Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie. ▪ Rozwiązanie musi posiadać możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego. ▪ Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj. ▪ Rozwiązanie musi posiadać możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji. ▪ Rozwiązanie musi posiadać możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet. ▪ Rozwiązanie musi wykrywać modyfikację w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu. ▪ Rozwiązanie musi posiadać możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. ▪ Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci. ▪ Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. ▪ Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie. ▪ Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość 	TAK	
----	--	-----	--

	<p>definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.</p> <ul style="list-style-type: none"> ▪ Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci. ▪ Rozwiązanie musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów: <ul style="list-style-type: none"> – z aplikacją lokalną, którą administrator wskazuje z listy, – z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP. 		
Kontrola dostępu do stron internetowych			
1.	<ul style="list-style-type: none"> ▪ Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. ▪ Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory. ▪ Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. ▪ Podstawowe kategorie, w jakie rozwiązanie musi być wyposażone to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. ▪ Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych. ▪ Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta. ▪ Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych. ▪ Rozwiązanie musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj. ▪ Rozwiązanie musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej. 	TAK	
Bezpieczna przeglądarka			
1.	<ul style="list-style-type: none"> ▪ Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. ▪ Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 	TAK	

	<ul style="list-style-type: none"> Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki. Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę. Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 		
Ochrona serwera Windows			
1.	<ul style="list-style-type: none"> Rozwiązanie musi posiadać wsparcie dla systemów Microsoft Windows Server 2008 R2 i nowszych. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. Rozwiązanie musi zapewniać pełną 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 posiadać wbudowaną technologię do ochrony przed rootkitami. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. Rozwiązanie ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocessorowych. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. Rozwiązanie musi posiadać możliwość 	TAK	

<p>umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.</p> <ul style="list-style-type: none"> ▪ Rozwiązanie musi wspierać mechanizm klastrowania. ▪ Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS). ▪ Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: <ul style="list-style-type: none"> – 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. ▪ Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. ▪ Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. ▪ Rozwiązanie musi posiadać zaawansowany skaner pamięci. ▪ Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej w czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych. ▪ Rozwiązanie musi oferować możliwość skanowania dysków sieciowych typu NAS. ▪ Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze. ▪ Rozwiązanie musi umożliwiać administratorowi 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. ▪ Funkcja 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. 		
---	--	--

<ul style="list-style-type: none"> ▪ Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. ▪ Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia. ▪ Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. ▪ Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. ▪ W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. ▪ Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. ▪ Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. ▪ Dodanie automatycznych wyłączeń nie wymaga restartu serwera. ▪ Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. ▪ Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. ▪ Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. ▪ Rozwiązanie ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). ▪ Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. ▪ Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. ▪ Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie. ▪ Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może 		
--	--	--

	<p>wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.</p> <ul style="list-style-type: none"> ▪ Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. ▪ Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. ▪ W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail. ▪ Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. ▪ Rozwiązanie musi posiadać możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło. ▪ Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo. ▪ Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiegś aktualizacji – poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji. ▪ Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje ▪ krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. ▪ Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń. ▪ System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. ▪ System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. ▪ Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, 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. ▪ Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzone dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. ▪ Rozwiązanie musi oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego 		
--	--	--	--

	<p>procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.</p> <ul style="list-style-type: none"> ▪ Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. ▪ Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera. ▪ Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji. ▪ Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. ▪ Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. ▪ Rozwiązanie musi być wyposażone w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). ▪ Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). ▪ Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. ▪ Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. ▪ Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania. ▪ Rozwiązanie musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”. ▪ Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. ▪ Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia. ▪ Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. ▪ Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. ▪ Rozwiązanie musi posiadać ochronę przed przyłączeniem komputera do sieci botnet. ▪ Rozwiązanie musi mieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. ▪ Rozwiązanie musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie 		
--	---	--	--

	<p>z wyłączeniem dokumentów.</p> <ul style="list-style-type: none"> Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 		
Administracja zdalna			
1.	<ul style="list-style-type: none"> Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019 oraz systemach Linux. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego 	TAK	

	<p>identyfikatora sprzętowego stacji.</p> <ul style="list-style-type: none"> ▪ Serwer administracyjny musi posiadać wsparcie dla „VDI” oraz „Golden Master Image”. ▪ Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów. ▪ Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy. ▪ Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. ▪ Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. ▪ Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS. ▪ Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP. ▪ Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11. ▪ Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap. ▪ Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych. ▪ Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów. ▪ Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. ▪ Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. ▪ Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android. ▪ Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS. ▪ Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zaporę osobistą, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci. ▪ Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. ▪ Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie 		
--	--	--	--

<p>zabezpieczające.</p> <ul style="list-style-type: none"> ▪ Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, 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 dla systemów Windows oraz MacOS z możliwością jego odinstalowania. ▪ Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. ▪ Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny. ▪ W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play. ▪ Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. ▪ Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzeniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS. ▪ Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego. ▪ Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi. ▪ Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. ▪ Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. ▪ Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. ▪ Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej. ▪ Serwer administracyjny musi posiadać 		
---	--	--

<p>możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.</p> <ul style="list-style-type: none"> ▪ Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej. ▪ Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji. ▪ Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych. ▪ Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. ▪ Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej. ▪ Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. ▪ Serwer administracyjny 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. ▪ Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania. ▪ Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. ▪ Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta. ▪ Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej. ▪ Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji. ▪ Z poziomu konsoli musi istnieć możliwość skalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce. ▪ Serwer administracyjny musi posiadać 		
---	--	--

	<p>minimum 120 szablonów raportów, przygotowanych przez producenta.</p> <ul style="list-style-type: none"> ▪ Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów. ▪ Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie. ▪ Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy. ▪ Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania. ▪ Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów. ▪ Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostęp do najbardziej interesujących danych. Panel ten musi być edytowalny. ▪ Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może <ul style="list-style-type: none"> ▪ zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF lub CSV. ▪ Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. ▪ Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów. ▪ Powiadomienia mailowe mają być wysyłane w formacie HTML. ▪ Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń. ▪ Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. ▪ Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu. ▪ Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji. ▪ Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami. ▪ Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych. ▪ W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji 		
--	---	--	--

	<p>produktu.</p> <ul style="list-style-type: none"> ▪ Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela. ▪ Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan. ▪ Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami. ▪ Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli. ▪ W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych. ▪ Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta. ▪ Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli. ▪ Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania. ▪ Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie. ▪ Konsola administracyjna musi umożliwiać personalizację interfejsu webowego. ▪ Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych. ▪ 9Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault). ▪ Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk. ▪ Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal). ▪ Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów. 		
--	---	--	--

Sandbox w chmurze

1.	<ul style="list-style-type: none"> 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. Analiza pliku może zakończyć się z wynikiem: <ul style="list-style-type: none"> Czysty, Podejrzany, Bardzo podejrzany, Szkodliwy. 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 próbki. 	TAK	
----	--	-----	--

Endpoint Detection and Response

	<p>Serwer</p> <ul style="list-style-type: none"> Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. System musi współpracować z serwerem administracyjnym produktu antywirusowego, 		
--	--	--	--

<p>tego samego producenta.</p> <ul style="list-style-type: none"> ▪ Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. ▪ Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych. ▪ 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 ponad 800 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. ▪ Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne. ▪ 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. ▪ Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali. ▪ 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 		
---	--	--

<p>lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.</p> <ul style="list-style-type: none"> ▪ Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy. ▪ 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. ▪ Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal). ▪ Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. ▪ Konsola administracyjna musi mieć możliwość tagowania obiektów. ▪ Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli. ▪ Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci. ▪ Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell. ▪ Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł. <p>Agent</p> <ul style="list-style-type: none"> ▪ Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10 oraz Windows Server 2008/2012/2016/2019. ▪ Pełne wsparcie dla systemów macOS 10.12 i nowszych. ▪ Wsparcie dla 32 i 64-bitowej wersji systemu Windows. ▪ Agent musi współpracować z produktem antywirusowym tego samego producenta. ▪ Agent nie może działać bez produktu antywirusowego tego samego producenta. ▪ W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonanej przez agenta. ▪ Połączenie agenta do serwera zarządzającego musi być szyfrowane.
--

	<ul style="list-style-type: none"> Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane. 		
	Gwarancja 24 miesiące		

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowany jeden procesor min. 8-rdzeniowy, o częstotliwości bazowej min. 2.6GHz, klasy x86 dedykowane do pracy zaoferowanym serwerem.
RAM	Minimum 128GB min DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache, Line Sparing
Gniazda PCI	Minimum jeden sloty PCIe x16 generacji 4
Interfejsy sieciowe	Minimum 4 interfejsy sieciowe 10/25GbE SFP28
Dyski twarde	<p>Możliwość instalacji dysków SAS, SATA, SSD</p> <p>Zainstalowane 2 dyski SSD SATA o pojemności min. 960GB, 6Gb, Hot-Plug</p> <p>możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.</p> <p>Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.</p>
Kontroler RAID	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1 z cache oraz podtrzymaniem
Wbudowane porty	4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 600W każdy.
Bezpieczeństwo	<p>☑ Zatrask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony, nieautoryzowanego dostępu do dysków twardych.</p> <p>☑ Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</p> <p>☑ BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła</p> <p>Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</p> <p>☑ Moduł TPM 2.0</p> <p>☑ Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera</p> <p>Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem</p>
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.

Karta Zarządzania	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:</p> <ul style="list-style-type: none"> - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; - możliwość podmontowania zdalnych wirtualnych napędów; - wirtualną konsolę z dostępem do myszy, klawiatury; - wsparcie dla IPv6; - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; - możliwość obsługi przez dwóch administratorów jednocześnie; - wsparcie dla dynamic DNS; - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. - możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
Certyfikaty	Serwer musi posiadać deklarację CE.
Warunki gwarancji	<p>3 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.</p> <p>W przypadku awarii dyski zostają u Użytkującego.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Użytkującego.</p> <p>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p> <p>Możliwość rozszerzenia gwarancji przez producenta do 7 lat.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera</p>
Dokumentacja użytkownika	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>

2. Oprogramowanie do Inwentaryzacji aktywów i ich konfiguracji – ilość stanowisk 35

Nazwa producenta:

Nazwa i typ:

Zamawiający dopuszcza również rozwiązanie równoważne zgodne z poniższymi zapisami:

1. Architektura / budowa

1.1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 35 klientów jednocześnie.

1.2. Architektura / budowa:

1.2.1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie

usługi systemowej.

- 1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).
- 1.2.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.
- 1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.

1.3. Konfiguracja Architektury:

- 1.3.1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.
- 1.3.2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.

2. Wymagania systemowe

- 2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 .
- 2.2. Klient musi działać na systemach 32 i 64 bitowych: min. Windows Server 2019/2022, Windows 8.1/10/11.
 - 2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci min.: Opera, Chrome, FireFox
- 2.3. Serwer musi działać na systemach 64 bitowych min.: m.in. Windows Server 2019/2022, Windows 8.1/10/11.

2.5. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

3. Interfejsy

3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.

3.2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL

3.3. System zapewnia integrację z modelem LLM.

4. Funkcjonalności systemu zarządzania infrastrukturą IT

4.1. Funkcjonalność Klienta

4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkownika.

4.2. Funkcjonalność konsoli administracyjnej.

4.2.1. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.

4.2.2. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.

4.3. Funkcjonalność panelu pracownika

4.3.1. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.

4.4. Zarządzanie licencjami

4.4.1. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.

4.5. Wzorce aplikacji i pakietów

4.5.1. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycji Microsoft Office.

4.6. Inwentaryzacja sprzętu komputerowego i urządzeń.

4.6.1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń.

4.7. Inwentaryzacja urządzeń sieciowych.

4.7.1. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.

4.8. Inwentaryzacja sprzętu.

4.8.1. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.

4.9. Ochrona danych (DLP)

4.9.1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.

4.10. Zdalna administracja komputerami

4.10.1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.

4.11. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.

4.12. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.

4.13. Zarządzanie Poprawkami i Aktualizacjami

4.13.1. System musi zapewniać ciągłe monitorowanie i identyfikację brakujących aktualizacji systemowych i komponentów infrastruktury IT, oferując funkcje rozpoznawania niezainstalowanych poprawek, ich pobierania, oraz klasyfikacji. Musi umożliwiać aktualizacje bez zakłócania pracy

użytkowników, zarówno zbiorowo jak i indywidualnie, z opcją szybkiego przywrócenia poprzedniego stanu systemu poprzez odinstalowanie niechcianych poprawek. System powinien również umożliwiać pomijanie niechcianych poprawek i dostarczać szczegółowe raporty dotyczące stanu aktualizacji oraz urządzeń, które mogą wymagać restartu.

4.14. Zdalne Zarządzanie Zaporą (Firewall)

4.14.1. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.

4.15. Automatyzacja

4.15.1. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.

4.16. Zarządzanie magazynem IT

4.16.1. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.

4.17. Repozytorium

4.17.1. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.

4.18. Kody kreskowe

4.18.1. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.

4.19. Wysyłanie wiadomości

4.19.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.

4.20. System musi posiadać możliwość eksportu / importu treści.

4.21. Monitorowanie drukarek sieciowych i wydruków

4.21.1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.

4.22. Monitorowanie stron www

4.22.1. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.

4.23. Monitorowanie serwerów WWW

4.23.1. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.

4.24. Monitorowanie dziennika zdarzeń

4.24.1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.

4.25. System musi umożliwiać monitorowanie komunikatów Syslog.

4.26. Monitorowanie pracy komputerów

4.26.1. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.

4.27. Monitorowanie uprawnień ACL

4.27.1. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizację danych i filtry do zarządzania informacjami.

4.28. Monitorowanie sensorów

4.28.1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.

4.29. Repozytorium CMDB

4.29.1. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.

4.30. Worktime manager

4.30.1. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostępnienia w panelu pracownika.

4.31. Raportowanie i eksport danych

4.31.1. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien

także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.

4.32. System musi zapewnić interfejs API.

4.32.1. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.

4.33. Powiadomienia

4.33.1. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.

4.34. Bezpieczeństwo

4.34.1. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.

5. Wsparcie i pomoc

5.1.1. Pomoc techniczna

5.1.1.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.

5.1.1.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.

5.1.1.3. Czas trwania usługi SLA od dnia zakupu do **30.06.2026** r.

3. NAS Klasy Enterprise – 1 szt.

Nazwa producenta:

Nazwa i typ:

L.p.	PARAMETR / WARUNEK WYMAGANY	PARAMETR OFEROWANY – PODAĆ
1.	Architektura procesora 64-bitowy x86	
2.	Procesor min. 4-rdzeniowy/4-wątkowy procesor o taktowaniu bazowym 2.0 GHz , zwiększanym do 2,9 GHz	

3.	Koprocesor arytmetyczny FPU	
4.	Mechanizm szyfrowania (AES-NI)	
5.	Transkodowanie wspomagane sprzętowo	
6.	Pamięć systemowa min. 8 GB RAM	
7.	Pamięć flash min. 4 GB (ochrona systemu operacyjnego przed podwójnym rozruchem)	
8.	Wnęka dysków min. 12 dyski 3,5-calowe SATA 6 Gb/s, 3 Gb/s	
9.	Kompatybilność dysków 3,5-calowe zatoki: 3,5-calowe dyski twarde SATA 2,5-calowe dyski SSD SATA	
10.	Wymieniany podczas pracy	
11.	Gniazdo M.2 poprzez kartę PCIe	
12.	Obsługa przyspieszenia pamięci podręcznej SSD	
13.	Port 2,5 Gigabit Ethernet (2,5G/1G/100M) min. 2 porty	
14.	Port 5 Gigabit Ethernet (5G/2,5G/1G/100M) poprzez kartę PCIe	
15.	Port 10 Gigabit sieci Ethernet Zainstalowana karta 2x 10GB sfp+ , należy dostarczyć 4 wkładki sfp+ SR , oraz niezbędne okablowanie	
16.	Wake on LAN (WOL)	
17.	Ramka Jumbo	
18.	Port USB 2.0 min. 2	
19.	Port USB 3.2 Gen 2 (10 Gb/s) min. 2	
20.	Montaż maks. 2U	
21.	liczba połączeń współbieżnych (CIFS) — z maks. pojemnością pamięci min. 1500	
22.	Wielkość puli min. 308 TB	
23.	Ilość storage-puli min. 128	
24.	Typy wolumenów Thick, Thin, Static	
25.	Wielkość wolumenu min. 250 TB	
26.	JBOD Expansio	
27.	VJBOD / VJBOD Cloud	
28.	iSCSI Service	
29.	Fibre Channel Service	
30.	LUN Type Thick, Thin	
31.	File-based iSCSI LUN	
32.	Block-based iSCSI LUN	
33.	Wielkość LUN min. 250 TB	
34.	Ilość targetów LUN min. 128	
35.	Funkcjonalności LUN: 1. LUN Mapping (LUN can be moved between iSCSI and FC) 2. LUN Masking 3. WWPN Aliases Import/Export 4. FC Port Group 5. FC Port Binding 6. Multipath IO (MPIO) 7. Online LUN capacity expansion 8. LUN snapshot 9. LUN snapshot replication and clone	
36.	Auto Tiering	

37.	Dyski Twarde SSD 4 szt. , Oferowane dyski twarde muszą znajdować się na liście kompatybilności producenta oferowanego NAS.	
	Typ dysku	SSD
	Format szerokości	2,5" (SFF)
	Typ napędu	Wewnętrzny
	Pojemność dysku min.	1.92 TB
	Interfejs dysku	SATA III - 6 Gb/s
	TBW	3504 TB
	Prędkość odczytu min.	560 MB/s
	Prędkość zapisu min.	530 MB/s
	Ilość operacji odczytu IOPS (min.)	94 K
	Ilość operacji zapisu IOPS (min.)	78 K

38.	Dyski Twarde Talerzowe 6 szt., Oferowane dyski twarde muszą znajdować się na liście kompatybilności producenta oferowanego NAS.	
	Typ dysku	HDD
	Format szerokości	3,5" (LFF)
	Typ napędu	Wewnętrzny
	Pojemność dysku min.	12 TB
	Interfejs dysku	SATA III - 6 Gb/s
	Prędkość obrotowa min.	7200 obr/min
	Bufor min.	256 MB
	Wielkość sektora dysku	4Kn
	Ilość operacji odczytu IOPS (min.)	170 K
	Ilość operacji zapisu IOPS (min.)	550 K
	Czas pracy pomiędzy awariami (MTBF)	2500000 h
	Nieprzerwana praca 24/7	Tak
	Pobór mocy maks.	8.6 W
	Pobór mocy maks. (czuwanie)	4.4 W
Oferowany NAS oraz dyski muszą być objęte 5-cio letnią gwarancją .		

1. NAS – 1 szt.

Nazwa producenta:

Nazwa i typ:

L.p.	PARAMETR / WARUNEK WYMAGANY	PARAMETR OFEROWANY – PODAĆ
1.	Architektura procesora 64-bitowy x86	
2.	Procesor min. 2-rdzeniowy/2-wątkowy o taktowaniu bazowym 2.0 GHz , zwiększanym do 2,9 GHz	
3.	Koprocesor arytmetyczny FPU	
4.	Mechanizm szyfrowania (AES-NI)	
5.	Transkodowanie wspomagane sprzętowo	
6.	Pamięć systemowa min. 4 GB RAM	

7.	Pamięć flash min. 4 GB (ochrona systemu operacyjnego przed podwójnym rozruchem)	
8.	Wnęka dysków min. 2 dysków 3,5-calowych SATA 6 Gb/s s	
9.	Kompatybilność dysków 3,5-calowe zatoki: 3,5-calowe dyski twarde SATA 2,5-calowe dyski SSD SATA	
10.	Wymieniany podczas pracy	
11.	Gniazdo M.2 2 x M.2 2280 PCIe Gen 3 x1	
12.	Obsługa przyspieszenia pamięci podręcznej SSD	
13.	Port 2,5 Gigabit Ethernet (2,5G/1G/100M) min. 1 porty	
14.	Port 5 Gigabit Ethernet (5G/2,5G/1G/100M) poprzez kartę PCIe	
15.	Port 10 Gigabit sieci Ethernet poprzez kartę PCIe	
16.	Wake on LAN (WOL)	
17.	Ramka Jumbo	
18.	Port USB 2.0 min. 2	
19.	Port USB 3.2 Gen 2 (10 Gb/s) min. 2	
20.	Kształt Tower	
21.	Gniazdo bezpieczeństwa Kensington	
22.	Liczba połączeń współbieżnych (CIFS) — z maks. pojemnością pamięci min. 1500	
23.	Gwarancja 2 lata	
24.	Dyski Twarde Talerzowe 2 szt.	
	Typ dysku	HDD
	Format szerokości	3,5" (LFF)
	Typ napędu	Wewnętrzny
	Pojemność dysku min.	12 TB
	Interfejs dysku	SATA III - 6 Gb/s
	Prędkość obrotowa min.	7200 obr/min
	Bufor min.	256 MB
	Oferowany NAS oraz dyski muszą być objęte 2 letnią gwarancją .	

5. Szkolenie dla pracowników IT

Zamawiający wymaga przeprowadzenia szkoleń z produktu firewall Fortigate stacjonarnie min. 8 godzin dla pracowników działu IT.

Program szkolenia musi obejmować min. :

- Wprowadzenie i wstępna konfiguracja
- Polityki zapory sieciowej
- Translacja adresów sieciowych (NAT)
- Uwierzytelnianie użytkowników

- Logowanie i monitoring
- Operacje oparte na certyfikatach
- Filtr stron www
- Kontrola aplikacji
- Antywirus
- System ochrony przed włamaniami i atakami DoS
- Koncepcja Security Fabric

Trener przeprowadzający szkolenie musi posiadać min. certyfikat:

- NSE4 - Network Security Professional
- NSE7 - Network Security Architect Enterprise Firewall
- Cisco Certified Network Professional Security

Certyfikaty należy dołączyć do oferty.

System EDR

Szkolenie stacjonarne w wymiarze min. 4 godziny.

Program szkolenia musi obejmować min. :

- tworzenie reguł
- tworzenie blokad urządzeń usb - oraz dopuszczanie wybranych
- update środowiska oraz hostów
- analiza logów systemu EDR
- w ramach szkolenia należy przekazać wiedzę niezbędną do samodzielnego zarządzania przez administratora zamawiającego

Narzędzie do inwentaryzacji zasobów

Szkolenie stacjonarne w wymiarze min. 4 godziny.

Program szkolenia musi obejmować min. :

- zdalne wdrażanie klienta programu
- tworzenie reguł
- tworzenie blokad urządzeń usb - oraz dopuszczanie wybranych
- update środowiska oraz hostów
- przechwytywanie sesji , działania związane w wymianą plików , oraz komunikatów ,
- w ramach szkolenia należy przekazać wiedzę niezbędną do samodzielnego zarządzania przez administratora zamawiającego

Wymagania w zakresie instalacji i konfiguracji dostarczanego sprzętu i oprogramowania :

1. Montaż serwerów w posiadanej szafie rack 42U w pomieszczeniu udostępnionym przez Zamawiającego.
2. Podłączenie serwera i NAS-a do listw zasilających PDU.
3. Aktualizacja oprogramowania układowego wszystkich komponentów.
4. Konfiguracja RAID serwera.
5. Instalacja i konfiguracja systemu operacyjnego.

6. Konfiguracja systemu zdalnego zarządzania.
7. Instalacja , uruchomienie i konfiguracja systemu backupowego na NAS.
8. Opracowanie polityki backupu .
9. Wymagane jest wykonanie testowego backupu oraz odtworzenia z weryfikacją prawidłowości działania systemów odtworzonych .
10. Wykonawca po zainstalowaniu i skonfigurowaniu sprzętu i oprogramowania będzie miał obowiązek przeprowadzenia instruktażu dla administratorów Zamawiającego w zakresie konfiguracji i zarządzania dostarczonego sprzętu oraz oprogramowania.