



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Numer sprawy: IZP.271.23.2025

Szczegółowy Opis Przedmiotu Zamówienia

na dostawę sprzętu i oprogramowania informatycznego związaną z realizacją
projektu w ramach grantu Cyberbezpieczny Samorząd



Cyberbezpieczny
Samorząd

Spis treści

1. Zestawienie ilościowe.....	3
2. Zasada równoważności rozwiązań i neutralności technologicznej.	4
3. Przedmiot zamówienia dla części nr 1.....	7
3.1. Wymagania ogólne.....	7
3.2. Zakup serwera (1 szt.).	9
3.3. Zakup przełącznika sieciowego TYP A (1 szt.).....	11
3.4. Zakup przełącznika sieciowego TYP B (1 szt.).....	12
3.5. Zakup UTM do klastra (1 szt.).....	13
3.6. Zakup usług konfiguracji środowiska IT (1 szt.).	19
4. Opis przedmiotu zamówienia części nr 2.	21
4.1. Wymagania ogólne.....	21
4.2. Zakup oprogramowania do zarządzania infrastrukturą IT (1 szt.).....	25
4.3. Rozbudowa oprogramowania antywirusowego o funkcje EDR (1 szt.).....	32
4.4. Zakup oprogramowania backup (1 szt.).	38

1. Zestawienie ilościowe.

Część nr 1 – Dostawa sprzętu i oprogramowania informatycznego.

Lp.	Nazwa	Ilość
1.	Zakup serwera	1 szt.
2.	Zakup przełącznika sieciowego TYP A	1 szt.
3.	Zakup przełącznika sieciowego TYP B	1 szt.
4.	Zakup UTM do klastra	1 szt.
5.	Zakup usług konfiguracji środowiska IT	1 szt.

Część nr 2 – Dostawa oprogramowania informatycznego.

Lp.	Nazwa	Ilość
1.	Zakup oprogramowania do zarządzania infrastrukturą IT	1 szt.
2.	Rozbudowa oprogramowania antywirusowego o funkcje EDR	1 szt.
3.	Zakup oprogramowania backup	1 szt.

2. Zasada równoważności rozwiązań i neutralności technologicznej.

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań lub też stosowane jest w celu wskazania aktualnie użytkowanego środowiska Zamawiającego, z którym rozwiązanie równoważne powinno być kompatybilne.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne. Wykonawca, który złoży ofertę na produkty równoważne musi do oferty załączyć dokumenty zawierające dokładny opis oferowanych produktów, z którego wynikać będzie zachowanie warunków równoważności. Wykonawca, który posługuje się równoważnymi certyfikatami musi je załączyć do oferty. Przez certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu z certyfikatami wskazanymi z nazwy, który potwierdza spełnianie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do wystawiania certyfikatów.
5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.
9. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia poprawności przeprowadzonych testów może wezwać

Wykonawcę do przedstawienia wskazanego przez Zamawiającego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowania overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.

10. W przypadku wskazania przez Zamawiającego określonych testów wydajności Zamawiający dopuszcza równoważne im testy wydajnościowe umożliwiające potwierdzenie zakładanych poziomów wydajności. W przypadku użycia przez Wykonawcę równoważnych testów wydajności Zamawiający zastrzega, iż w celu sprawdzenia równoważności przeprowadzonych testów Wykonawca może zostać wezwany do dostarczenia Zamawiającemu wskazanego przez Zamawiającego oprogramowania testującego i równoważnego do niego oprogramowania testującego wraz z testowanym urządzeniem i/lub oprogramowaniem. Wszystkie testy wydajnościowe wykonawca musi przeprowadzić w oferowanej konfiguracji, przy automatycznych ustawieniach konfiguratora oprogramowania testującego i natywnej rozdzielczości wyświetlacza oraz włączonych wszystkich urządzeniach. Nie dopuszcza się stosowania overclockingu, oprogramowania wspomagającego pochodzącego z innego źródła niż fabrycznie zainstalowane oprogramowanie przez producenta, ingerowania w ustawieniach BIOS (tzn. wyłączanie urządzeń stanowiących pełną konfigurację), jak również w samym środowisku systemu (tzn. zmniejszanie rozdzielczości, jasności i kontrastu itp.). Zamawiający dopuszcza prowadzenie testów wydajnościowych w oparciu o dowolny system operacyjny zainstalowany na urządzeniu.
11. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych (zwana dalej ustawą), Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych takich samych lub lepszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.) jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów / produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia dopuszcza rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne

opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów uwiarygodniających te rozwiązania.

3. Przedmiot zamówienia dla części nr 1.

3.1. Wymagania ogólne.

1. Dostarczony sprzęt i oprogramowanie muszą być wolne od wad prawnych i fizycznych oraz nienoszący oznak użytkowania.
2. Dostarczony sprzęt i oprogramowanie muszą być fabrycznie nowe (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), muszą pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu i oprogramowania.
3. Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale”, „end-of-support”, „end-of-life” producenta lub innych listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.
4. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów. Niedopuszczalna jest realizacja tylko części funkcji bądź wymaganych standardów zamiast innych określonych jako minimalne w niniejszym dokumencie. Wszystkie wymagania minimalne muszą zostać zapewnione przez dostarczane produkty bez konieczności zakupu żadnych dodatkowych elementów przez Zamawiającego, chyba że z niniejszego dokumentu wynika inaczej.
5. Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
6. Wykonawca zapewni dostawę do wskazanej lokalizacji przez Zamawiającego.
7. Wykonawca jest odpowiedzialny za skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzeń do działania, pozwalające na rozpoczęcie pracy oraz dostarczenie odpowiedniej ilości kabli zasilających, połączeniowych w celu przygotowania zamawianego sprzętu do działania. Wykonawca jest zobowiązany dostarczyć wszelkie okablowanie, wkładki, organizery, listy zasilające, opaski zaciskowe, kable połączeniowe pomiędzy sprzętami łącząc je z istniejącą infrastrukturą Zamawiającego.
8. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
9. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
10. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
11. Dla dostaw sprzętu informatycznego z oprogramowaniem Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania (w tym systemu operacyjnego) nieużywanego oraz nigdy wcześniej nieaktywowanego na innym urządzeniu oraz pochodzącego z legalnego źródła sprzedaży. W

przypadku oprogramowania naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania (faktury, rachunki) w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

12. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.

3.2. Zakup serwera (1 szt.).

Minimalne parametry techniczne serwera:

1. Obudowa typu RACK o wysokości maksymalnie 2U z możliwością instalacji min. 8 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie RACK i wysuwanie serwera do celów serwisowych.
2. Płyta główna z możliwością zainstalowania dwóch procesorów.
3. Zainstalowany jeden procesor klasy x86 dedykowany do pracy z oferowanym serwerem, umożliwiający osiągnięcie przez serwer wyniku co najmniej 380 punktów w teście SPECrate2017_fp_base dla konfiguracji dwuprocesorowej według wyników publikowanych na stronie www.spec.org. Zamawiający żąda załączenia do oferty przedmiotowego środka dowodowego określonego w SWZ potwierdzającego spełnienie dla procesora dedykowanego do pracy z zaoferowanym serwerem żądanej przez Zamawiającego wydajności.
4. Pamięć RAM: zainstalowane min. 128 GB w najnowszej technologii oferowanej przez producenta, płyta główna musi obsługiwać do min. 1 TB pamięci RAM DDR5, co najmniej 12 slotów na pamięć wolnych w oferowanej konfiguracji.
5. Zabezpieczenia pamięci RAM: Memory Rank Sparing i/lub Memory Mirror i/lub Single Device Data Correction i/lub Memory Lockstep i/lub Chipkill i/lub Extended ECC i/lub Advanced Memory Device Correction i/lub AMD Memory Guard i/lub ECC i/lub Demand Scrubbing i/lub Patrol Scrubbing i/lub Permanent Fault Detection (PFD).
6. Zintegrowana karta graficzna ze złączem VGA.
7. Interfejsy sieciowe: Wbudowane co najmniej 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT, co najmniej 2 interfejsy sieciowe 10Gb Ethernet w standardzie 10GBase-T, co najmniej 2 interfejsy 25GbE w standardzie SFP28 z dedykowanymi wkładkami do każdego portu.
8. Dyski twarde: Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 2 dyski twarde Hot-Plug SSD SATA o prędkości min. 6 Gb/s o pojemności co najmniej 960 GB każdy. Dodatkowo zainstalowana karta wyposażona w dwa dyski M.2 NVMe o pojemności min. 480GB Hot-Plug skonfigurowana w RAID 1. W przypadku uszkodzenia dysku w okresie gwarancji Zamawiający wymaga by uszkodzony dysk pozostał jego własnością.
9. Kontroler RAID: Sprzętowy kontroler dyskowy umożliwiający konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
10. Wsparcie dla dysków samoszyfrujących.
11. Wbudowane porty: min. 3 porty USB, w tym co najmniej 1 port USB musi być dostępny z przodu obudowy. Ilość dostępnych portów USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgąęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera.
12. Wentylatory: typu Hot Plug.
13. Zasilacze: Redundantne typu Hot Plug o mocy nieprzekraczającej 1100 W każdy.
14. Karta/moduł zarządzania: Niezależny od zainstalowanego na serwerze systemu operacyjnego posiadający dedykowane złącze umożliwiające zdalne zarządzanie:
 - 1) zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
 - 2) zdalne monitorowanie i informowanie o statusie serwera,
 - 3) szyfrowane połączenie oraz autentykację i autoryzację użytkownika,
 - 4) możliwość podmontowania zdalnych wirtualnych napędów,

- 5) wirtualną konsolę z dostępem do myszy, klawiatury,
 - 6) wsparcie dla IPv6,
 - 7) wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH,
 - 8) integracja z Active Directory,
 - 9) wsparcie dla dynamic DNS.
15. System bezpieczeństwa serwera realizowany poprzez następujące zabezpieczenia:
- 1) wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera;
 - 2) blokada zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych;
 - 3) moduł TPM 2.0.
16. Wykonawca jest zobowiązany do dostawy wraz z serwerem systemu operacyjnego umożliwiającego zarządzanie serwerem klasy Microsoft Windows Server Standard 2025 wraz z 20 licencjami dostępowymi umożliwiającymi korzystanie przez 20 użytkowników z zasobów serwera lub równoważnego systemu zgodnie z poniżej określonymi warunkami równoważności.
- Warunki równoważności dla dostawy oprogramowania Microsoft Windows Server Standard 2025 wraz z 20 licencjami dostępowymi Microsoft Windows Server 2025 CAL User:
- 1) Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i czterech wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji oraz dostępu do serwerowego systemu operacyjnego dla minimum 20 użytkowników.
 - 2) Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
 - 3) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
 - 4) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
 - 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
 - 6) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
 - 7) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
 - 8) Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
 - 9) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
 - 10) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
 - 11) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
 - 12) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
 - 13) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

- 14) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
 - 15) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
 - 16) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
 - 17) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
 - 18) Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
 - 19) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
 - 20) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
17. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025.
18. Jakość produktu i sposobu jego wykonania: Certyfikat ISO 9001 lub inny równoważny dokument poświadczający, że producent serwera opracował, wdrożył i certyfikował system zarządzania jakością; Certyfikat ISO 50001 lub ISO 14001 lub inny równoważny dokument poświadczający, że producent serwera posiada system zarządzania energią, zmniejszający zużycie energii, wpływy na środowisko i zwiększający rentowność; Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany serwer spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE; Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany serwer i jego/ich producenta/producentów wymagań w zakresie określonym powyżej.
19. Gwarancja: min. 60 miesięcy gwarancji producenta obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji realizowanej w miejscu instalacji sprzętu z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, w przypadku awarii dyski Zamawiający wymaga, aby dyski pozostały u Zamawiającego. Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta lub dedykowany portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji przez portal producenta serwera. Gwarancja powinna rozpocząć swój bieg od dnia podpisania końcowego protokołu odbioru całego zamówienia.

3.3. Zakup przełącznika sieciowego TYP A (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Rodzaj urządzenia: zarządzalny przełącznik L2.
2. Rodzaj obudowy: umożliwiający montaż w szafie RACK (wraz z kompletem szyn/wieszaków do montażu w szafie RACK).

3. Przepustowość routowania/przełączania: min. 600 Gbit/s.
4. Prędkość przekazywania: min. 450 Mpps.
5. Bufor pamięci dla pakietów: min. 2 MB.
6. Rozmiar tablicy MAC: min. 32 000 wpisów.
7. Dostępne interfejsy: min. 24x 1/10GBase-X SFP+ oraz minimum 2x 40GBase-X QSFP.
8. Obsługiwane standardy komunikacyjne: IEEE 802.1Q; IEEE 802.3ad; IEEE 802.1D; IEEE 802.1w; IEEE 802.1s; IEEE 802.1x; IEEE 802.1p; IEEE 802.3ah; 802.1ag;
9. Obsługiwane protokoły zarządzające: SNMPv1, SNMPv2, SNMPv3, RMON.
10. Obsługiwane protokoły sieciowe: IPv4, IPv6, LLDP, MSTP, RSTP, Telnet, TACACS+, MLD.
11. Inne cechy: zarządzanie przez www, generowanie raportów zdarzeń systemowych, obsługa min. 4000 sieci VLAN, obsługa multicast, funkcję agregacji portów z wykorzystaniem protokołu LACP, uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia; obsługa list kontroli dostępu (ACL).
12. Możliwość łączenia urządzeń w stos min. 4.
13. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany przełącznik sieciowy spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta przełącznika sieciowego lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany przełącznik wymagań w zakresie określonym powyżej.
14. Co najmniej 60 miesięcy gwarancji producenta.

3.4. Zakup przełącznika sieciowego TYP B (1 szt.).

Minimalne parametry techniczne urządzenia:

1. Rodzaj urządzenia: zarządzalny przełącznik L2.
2. Rodzaj obudowy: umożliwiający montaż w szafie RACK (wraz z kompletem szyn/wieszaków do montażu w szafie RACK).
3. Przepustowość routowania/przełączania: min. 170 Gbit/s.
4. Prędkość przekazywania: min. 130 Mpps.
5. Bufor pamięci dla pakietów: min. 2 MB.
6. Rozmiar tablicy MAC: min. 16 000 wpisów.
7. Dostępne interfejsy: min. 48 x 10/100/1000Base-T RJ45 oraz minimum 4x 1/10GBase-X SFP+.
8. Obsługiwane standardy komunikacyjne: IEEE 802.1Q; IEEE 802.3ad; IEEE 802.1D; IEEE 802.1w; IEEE 802.1s; IEEE 802.1x; IEEE 802.1p; IEEE 802.3ah; 802.1ag;
9. Obsługiwane protokoły zarządzające: SNMPv1, SNMPv2, SNMPv3, RMON.
10. Obsługiwane protokoły sieciowe: IPv4, IPv6, LLDP, MSTP, RSTP, Telnet, TACACS+, MLD.
11. Inne cechy: zarządzanie przez www, generowanie raportów zdarzeń systemowych, obsługa min. 4000 sieci VLAN, obsługa multicast, funkcję agregacji portów z wykorzystaniem protokołu LACP, uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia; obsługa list kontroli dostępu (ACL).

12. Możliwość łączenia urządzeń w stos min. 4.
13. Jakość produktu i sposobu jego wykonania: Deklaracja zgodności CE lub inny równoważny dokument poświadczający, że oferowany przełącznik sieciowy spełnia wszystkie zasadnicze wymagania zawarte w poszczególnych dyrektywach nowego podejścia przewidujących oznakowanie CE. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta przełącznika sieciowego lub innego dokumentu potwierdzającego spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Zamawiający żąda załączenia do oferty przedmiotowych środków dowodowych - dokumentów potwierdzających spełnienie przez oferowany przełącznik wymagań w zakresie określonym powyżej.
14. Co najmniej 60 miesięcy gwarancji producenta.

3.5. Zakup UTM do klastra (1 szt.).

Przedmiotem zamówienia jest dostawa urządzenia UTM mogącego pracować w klastrze wysokiej dostępności (HA) w trybach Active/Standby, Active/Active z już posiadanym przez Zamawiającego urządzeniem PaloAlto – PA-440 z zapewnieniem usług dla klastra w postaci minimum Threat Prevention, VPN, Zaawansowane filtrowanie adresów URL, ochrona plików, DNS Security do dnia 30.06.2026 r. lub dostawa równoważnej redundantnej platformy bezpieczeństwa spełniającej minimalne kryteria równoważności określone poniżej.

Minimalne kryteria równoważności do dostawy urządzenia do klastra wraz z istniejącym urządzeniem (wymagania dotycząc jednego urządzenia):

1. Cechy urządzenia (parametry minimalne, muszą być spełnione dla każdego z dostarczanych urządzeń firewall):
 - a. Wysokość maksymalnie 1U wraz z zestawem montażowym do szafy RACK 19”,
 - b. Możliwość podłączenia redundantnego źródła zasilania,
 - c. 8 portów 1G Ethernet RJ45.
2. Rozwiązanie musi być wyposażone w co najmniej jeden port konsoli szeregowej RJ45, w co najmniej jeden dedykowany port zarządzający realizowany jako port 10/100/1000 Mbps Ethernet.
3. Obsługa (parametry minimalne, parametry wydajnościowe muszą być spełnione dla każdego z dostarczanych urządzeń firewall):
 - a. 2.2 Gbps przepustowości Firewall/kontroli aplikacji,
 - b. 1.0 Gbps przepustowości Firewall/kontroli aplikacji/IPS/Antywirus/Antymalware,
 - c. 180 000 jednoczesnych sesji,
 - d. 30 000 nowych połączeń na sekundę,
 - e. Lokalnej przestrzeni na system operacyjny i logi co najmniej o pojemności minimum 120GB.
4. Jako scenariusz firewall/kontroli aplikacji Zamawiający rozumie, iż rozwiązanie pozwoli na:
 - a. wykrycie aplikacji,
 - b. przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.
5. Jako scenariusz firewall/IPS/antywirus/kontroli aplikacji/antymalware Zamawiający rozumie, iż rozwiązanie pozwoli na:

- a. wykrycie aplikacji,
 - b. przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych, inspekcje IPS, antywirus, antyspyware.
6. Zakres kontroli musi też obejmować przesyłanie plików do sandboxa lokalnego i chmurowego w tym przechwytywanie i blokowanie plików określonego typu.
7. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla rozwiązania sygnaturami IPS oraz z wszystkimi funkcjami dostępnymi w rozwiązaniu dla silników antywirus i antyspyware/antymalware.
8. Inspekcjom bezpieczeństwa musi podlegać cały ruch – sprawdzeniu musi podlegać każdy bajt danych przesyłany przez rozwiązanie.
9. Zamawiający wymaga, aby podana została przepustowość urządzenia dla pełnego zakresu ochrony oferowanego przez rozwiązanie – jeżeli rozwiązanie pozwala na pracę w wielu trybach, to należy podać przepustowość dla trybu z największą liczbą dostępnych inspekcji dla silników IPS, antywirus, antymalware/antyspyware.
10. Rozwiązanie musi spełniać co najmniej następujące parametry wydajnościowe odnośnie funkcjonalności site-to-site VPN:
 - a. minimum 1 Gbps dla IPSEC VPN
 - b. minimum 2500 tuneli IPSEC VPN (site-to-site).
11. Rozwiązanie musi spełniać co najmniej następujące parametry wydajnościowe odnośnie funkcjonalności remote access VPN:
 - a. minimum 900 tuneli VPN Remote Access z wykorzystaniem klienta VPN. Oprogramowanie klienta VPN musi być objęte wsparciem producenta.
 - b. minimum 90 tuneli tzw. Clientless VPN - bez konieczności zastosowania klienta.
12. Rozwiązanie musi obsługiwać nie mniej niż 3 wirtualnych routerów posiadających odrębne tabele routingu.
13. Musi mieć możliwość rozbudowy do 2 wirtualnych instancji firewall (określanych jako kontekst/domena/system). Każda z instancji musi pozwalać na konfigurację niezależnych oraz odrębnych od innych instancji – polityk bezpieczeństwa (co najmniej dla IPS, AV i współpracy z sandboxem), tablicy routingu oraz realizacji zdalnego dostępu.
14. Urządzenia muszą umożliwiać działanie w następujących trybach pracy:
 - a. rutera (tzn. w warstwie 3 modelu OSI),
 - b. mostu (tzn. w warstwie 2 modelu OSI),
 - c. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; Musi pracować w trybie przezroczystego łączenia interfejsów w pary.).
 - d. w trybie pasywnego nasłuchu (sniffer/tap).
15. System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
16. Urządzenia firewall muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu od zasobów służących do zarządzania urządzeniem.
17. Urządzenie musi posiadać dedykowane zasoby/rdzenie procesora/procesorów do funkcji zarządzania urządzeniem lub możliwość ustawienia dedykowanych zasobów/rdzeni procesora/procesorów do funkcji zarządzania urządzeniem.

18. Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.
19. Urządzenia firewall muszą wspierać protokół LACP.
20. Urządzenia firewall muszą zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
21. Urządzenia firewall muszą działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.
22. Polityka zabezpieczeń firewall musi uwzględniać
 - a. adresy IP źródłowe i docelowe,
 - b. protokoły i usługi sieciowe,
 - c. aplikacje,
 - d. kategorie URL,
 - e. użytkowników aplikacji i grupy,
 - f. reakcje zabezpieczeń,
 - g. logowanie zdarzeń (początek i koniec sesji)
 - h. strefa wejściowa i wyjściowa
23. Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65535 dostępnych portach. Przy tym wydajność kontroli firewalla stanowego i kontroli aplikacji całego ruchu nie może być mniejsza, niż wskazano w wymaganiach wydajnościowych urządzeń.
24. Urządzenie musi wykrywać co najmniej 3700 predefiniowanych aplikacji wspieranych przez producenta (takich jak DNS over HTTPS, Telegram, Skype, Tor, BitTorrent, MQTT, Modbus, DNP3, Siemens S7) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.
25. Urządzenia firewall muszą pozwalać na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.
26. Urządzenia firewall muszą zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.
27. Urządzenia firewall muszą być wyposażone w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Jeżeli dostęp do API, jego dokumentacji, zadawania pytań pomocy wymaga licencji lub subskrypcji – należy dostarczyć odpowiednie dla minimum 30 administratorów.

28. Dostęp do urządzeń i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
29. Urządzenia firewall muszą umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż:
 - a. baza lokalna,
 - b. serwer Radius,
 - c. serwer TACACS+,
 - d. serwer AD/LDAP.
30. Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH a dla dostępu GUI za pomocą certyfikatów kryptograficznych.
31. Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami:
 - a. Active Directory,
 - b. Terminal Services
32. Polityka kontroli dostępu (urządzeń firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości musi odbywać się również transparentnie.
33. Urządzenia firewall muszą pozwalać na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL.
34. Urządzenie musi dostarczać predefiniowane przez producenta raporty standardowe jak i możliwość tworzenia raportów niestandardowych. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu.
35. Urządzenie musi pozwalać na zapisanie raportów na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
36. Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykiet musi pozwalać na użycie:
 - a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia)
 - b. API
37. Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare ESX i VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można potem wykorzystywać w polityce bezpieczeństwa urządzeń.
38. Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF.
39. Urządzenia firewall muszą obsługiwać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
40. Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

41. Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami NAT.
42. Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju.
43. Urządzenia firewall muszą obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
44. Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa.
45. Wykonywanie operacji deszyfrowania ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji. Musi zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.
46. Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL.
47. Dla deszyfrowania ruchu TLS 1.3 wymagane jest wsparcie dla X25519, X448 oraz minimum dla zestawów protokołów: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384 oraz TLS_CHACHA20_POLY1305_SHA256.
48. Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
49. Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) i ustawiania dla aplikacji priorytetu oraz pasma.
50. Urządzenia firewall muszą umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPsec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia trasowania (tzw. routing-based VPN).
51. Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
52. Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
53. Urządzenia firewall muszą zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tuneli SSH.
54. Urządzenia firewall muszą posiadać funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (nazywany często również jako IPS). Baza sygnatur IPS/IDS musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
55. Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur albo powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła.
56. Urządzenia firewall muszą posiadać funkcję ręcznego tworzenia sygnatur (IPS) bezpośrednio na urządzeniu.
57. Urządzenia firewall muszą posiadać funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół minimum: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż raz na 48 godzin i pochodzić od tego samego producenta co firewall.
58. Urządzenia firewall muszą posiadać funkcję anty-spyware. Baza sygnatur musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall.

59. Rozwiązanie musi posiadać możliwość analizy nieznanej komunikacji C2 (command-and-control) oraz spyware w oparciu o nauczanie maszynowe realizowane w czasie rzeczywistym, przy czym:
- a. musi być możliwe jest blokowanie wykrytej komunikacji C2 w czasie rzeczywistym,
 - b. powyższe musi być możliwe minimum dla ruchu typu: HTTP, HTTP/2, SSL oraz niezidentyfikowanych przez urządzenie aplikacji w ruchu TCP i UDP.
60. Urządzenia firewall muszą posiadać funkcję filtrowania URL.
61. Funkcja filtrowania URL musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
62. Rozwiązanie musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania kategorii URL.
63. Urządzenia firewall muszą umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „SandBox” plików wykonywalnych PE i DLL przechodzących przez firewall. Systemy sandbox, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików, adresów IP, DNS i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik. Maksymalny interwał aktualizacji sygnatur 48 godzin.
64. System zabezpieczeń NGFW musi dodatkowo oferować możliwość identyfikacji w ruchu sieciowym i przesyłania do zintegrowanej usługi analizy dynamicznej (tzw. „sandbox”) plików następujących typów: wykonywalnych (PE), Microsoft Office, Adobe flash / PDF, archiwa: JAR, RAR, 7-ZIP, Android APK, Mac OSX, skrypty: BAT, JScript, PowerShell, VBS, Perl i Python. W przypadku potwierdzenia nieznanego ataku (tzw. „zero-day”), musi następować automatyczna aktualizacja systemu firewall nowymi sygnaturami opisującymi wykryte pliki malware lub ich zidentyfikowane złośliwe zachowania (np. wzorce komunikacji zwrotnej) w wyniku przeprowadzonej analizy.
65. Uruchomienie ochrony typu „sandbox” dla systemu zabezpieczeń NGFW musi być możliwe w następujących trybach:
- a. Subskrypcji - bez dokupowania jakichkolwiek komponentów sprzętowych wyłącznie w oparciu o usługę chmurową producenta rozwiązania
 - b. Prywatnym - po zakupieniu dodatkowego urządzenia do analizy lokalnej
 - c. Hybrydowym - z wykorzystaniem zarówno subskrypcji i po zakupieniu urządzenia do analizy lokalnej
66. W każdym z powyższych trybów, administrator systemu NGFW musi mieć możliwość konfiguracji rodzaju pliku, kontekstu użytej aplikacji, kierunku transmisji (wysyłanie / odbieranie) i miejsca analizy (chmura / urządzenie lokalne) dla celów definicji ruchu i klasyfikacji obiektów do analizy typu „sandbox”.
67. Zintegrowana z rozwiązaniem NGFW subskrypcja „sandbox” powinna mieć udokumentowane wsparcie producenta dla najnowszych technik analizy złośliwego oprogramowania:
- a. wykorzystanie własnego, utwardzonego hypervisor-a, względem potencjalnych metod rozpoznawania generycznego środowiska wirtualnego przez malware,
 - b. automatyczne rozpakowanie malware-u zaciemnionego metodami kompresji (tzw. packer-ów) celem pełnej widoczności zachowania jego kodu,
 - c. emulacja zależności wymaganych przez potencjalnie złośliwe oprogramowanie do jego pełnego uruchomienia w środowisku piaskownicy,
 - d. tworzenie zrzutów pamięci dla potencjalnie złośliwych zachowań podczas wykonywania kodu jako sposobu monitorowania środowiska piaskownicy i ich uwzględnienia w werdykcie końcowym.

68. Urządzenia firewall muszą umożliwiać zabezpieczenie działania protokołu DNS poprzez procesowanie zapytań DNS w celu wykrywania i blokowania: zagrożeń, wycieku danych (exfiltracja), tunelowania DNS. Urządzenia muszą posiadać ciągły (on-line) dostęp do centralnego repozytorium zagrożeń DNS, który będzie wykorzystywany w procesie decyzyjnym funkcjonalności.
69. System zabezpieczeń firewall musi być wyposażony w mechanizm automatycznego wyboru optymalnego trasowania WAN dla zdefiniowanej aplikacji, przy zapewnieniu jej maksymalnej wydajności, dostępności oraz bezpieczeństwa. Dla różnych technologii połączeń fizycznych WAN (np. LTE, DSL, MPLS, WiFi itd.) zakończonych w standardzie Ethernet, musi być możliwość ich ciągłego monitorowania w zakresie: straty pakietów, opóźnień oraz odchylenia (tzw. jitter) jako parametrów decyzyjnych do dynamicznego wyboru najkorzystniejszej trasy. Zintegrowana funkcjonalność SD-WAN, musi działać bezpośrednio na urządzeniu, w oparciu o system centralnego zarządzania, bez konieczności dokupywania dodatkowych komponentów, poza subskrypcją.
70. System zabezpieczeń NGFW musi posiadać osobny zestaw polityk SD-WAN, definiujący najkorzystniejszy sposób dystrybucji kluczowego ruchu firmowego, rozdzielny od polityk bezpieczeństwa. Pojedyncza reguła SD-WAN musi uwzględniać następujące atrybuty ruchu: strefy bezpieczeństwa, adresy IP źródłowe i docelowe, aplikacje, porty usług, wartości klasyfikatorów jakościowych łącz (opóźnienie, strata pakietów, jitter) oraz metody korekcji błędów.

3.6. Zakup usług konfiguracji środowiska IT (1 szt.).

1. Zrealizowany zakres prac w zakresie minimum powinien polegać na: Montaż urządzeń w szafie rack; Podłączenie przewodów sieciowych i zasilających; Uruchomienie urządzeń, sprawdzenie parametrów, instalacja dostępnych na dzień wdrożenia aktualizacji; Konfiguracja ustawień; Podłączenie urządzeń NGFW; Konfiguracja i podłączenie przełączników; Instalacja serwera kopii zapasowej dla oprogramowania backupowego; Instalacja zapasowego kontrolera domeny; Konfiguracja kontrolera domeny.
2. W zakresie usług konfiguracji przełączników sieciowych Wykonawca będzie zobowiązany minimum do: Aktualizacja firmware do najnowszej wersji dostępnej w dniu instalacji; Ustawienie dostępu dla administratorów; Ustawienie interfejsu zarządzania; W przypadku urządzeń, gdzie możliwe jest zastosowanie protokołu VSF – wykonanie połączenia przewodami oraz konfiguracja systemu w taki sposób, by zarządzanie mogło odbywać się z jednego urządzenia; Konfiguracja L2 - 802.1Q vlan zgodnie z projektem; Konfiguracja L2 - 802.3 Link Aggregation with LACP zgodnie z projektem; Konfiguracja L2 - 802.1w RSTP zgodnie z projektem.
3. W zakresie konfiguracji HA zapory sieciowej Wykonawca będzie zobowiązany minimum do: Instalacja urządzeń w dedykowanym uchwycie rack w szafie sieciowej; Konfiguracja podstawowych interfejsów urządzenia zapasowego; Aktywacja, aktualizacja i konfiguracja urządzenia umożliwiającego konfigurację trybu HA; Uruchomienie usługi HA zgodnie z projektem na obu urządzeniach firewall; Synchronizacja konfiguracji między urządzeniami; Ustawienia monitorowania zdarzeń i reakcji na zdarzenia w funkcji HA; Testy przełączenia firewalla.
4. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia sprzętu i oprogramowania – wymagania minimalne:
 - a. Wykonawca przygotowuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego sprzętu

i oprogramowania po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:

- i. scenariusze testowe, procedury oraz wzory raportów testów,
 - ii. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
 - iii. opis koncepcji realizacji prac,
 - iv. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
- b. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:
- i. Wykonawca prześle do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 10 dni kalendarzowych od dnia zawarcia umowy,
 - ii. Zamawiający w terminie nie dłuższym niż 5 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
 - iii. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
 - iv. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
 - v. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
 - vi. zatwierdzony projekt techniczny wraz z procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
- c. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
- d. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
- e. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
- f. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery”. Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.
5. Instruktaże w zakresie dostarczonego sprzętu i oprogramowania – wymagania minimalne.

- a. Instruktaże stanowiskowe będą prowadzone w języku polskim w siedzibie Zamawiającego i obejmą zakresem m.in.: użytkowane oprogramowanie; budowę, architekturę i konfigurację rozwiązania; administrowanie wdrożonym rozwiązaniem.
- b. Instruktaże stanowiskowe zostaną przeprowadzone przez osoby prowadzące prace wdrożeniowe w ramach niniejszego zamówienia.
- c. Instruktaże powinny trwać minimum 8 godzin lekcyjnych (45 minut) i będą przeprowadzone dla wskazanej przez Zamawiającego liczby osób (maksymalnie 2 osoby).
- d. Zamawiający dopuszcza przeprowadzenia instruktaży w trybie zdalnym (online).
- e. Administratorzy rozwiązania po zakończeniu Instruktaży stanowiskowych muszą w szczególności umieć wykonywać czynności administracyjne, a także instalacji oprogramowania, znać i umieć realizować procedury backupu. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem rozwiązania, a także sposoby ich przeciwdziałania, wykrywania i usuwania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować wdrożone rozwiązanie, jak również znać jego wdrożoną konfigurację.

4. Opis przedmiotu zamówienia części nr 2.

4.1. Wymagania ogólne.

1. Dostarczone oprogramowanie musi być wolne od wad prawnych i fizycznych oraz nienoszące oznak użytkowania.
2. Dostarczone oprogramowanie musi być fabrycznie nowe, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego oprogramowania.
3. Niedopuszczalne są produkty prototypowe, oprogramowanie nie może znajdować się na liście „end-of-sale”, „end-of-support”, „end-of-life” producenta lub innych listach prowadzonych przez producentów produktów świadczących o tym, że produkt został wycofany ze sprzedaży, wsparcie dla niego zostało zakończone lub producent zaprzestaje wydawania aktualizacji, poprawek bezpieczeństwa czy też napraw dla produktu.
4. Wykonawca zapewni dostawę oprogramowania do wskazanej lokalizacji w siedzibie Zamawiającego.
5. Prace instalacyjne będzie można realizować wyłącznie w terminach uzgodnionych z Zamawiającym.
6. Wykonawca będzie zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i oprogramowania, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i oprogramowania.
7. Dla dostaw oprogramowania Zamawiający wymaga fabrycznie nowego oprogramowania (nieużywanego nigdy wcześniej), w wersji z certyfikatem autentyczności dla każdej licencji, o ile producent oferowanego oprogramowania stosuje certyfikaty autentyczności. Wykonawca zobowiązany jest do dostarczenia fabrycznie nowego oprogramowania, nieużywanego oraz nigdy wcześniej nieaktywowanego oraz pochodzącego z legalnego źródła sprzedaży. W przypadku oprogramowania posiadającego fizyczny nośnik naklejka hologramowa winna być zabezpieczona przed możliwością odczytania klucza za pomocą zabezpieczeń stosowanych przez producenta, o ile producent oferowanego oprogramowania stosuje takie zabezpieczenia. Zamawiający zastrzega

możliwość weryfikacji dostarczonego oprogramowania na etapie oceny ofert jak i na etapie dostawy pod kątem legalności oprogramowania bezpośrednio u producenta oprogramowania. Zamawiający zastrzega możliwość żądania od Wykonawcy na etapie dostawy przedstawienia dokumentów dotyczących zakupu oprogramowania w autoryzowanym kanale dystrybucyjnym producenta oprogramowania.

8. Wymagania instalacyjne i wdrożeniowe dla dostarczonego oprogramowania:
 - a. Instalacja ma odbyć się na komputerach oraz serwerach wskazanych przez Zamawiającego, a w przypadku jeżeli dostarczone oprogramowanie działa w modelu rozwiązania chmurowego to Wykonawca jest zobligowany do konfiguracji oprogramowania w chmurze Wykonawcy bądź Producenta oferowanego oprogramowania.
 - b. Zamawiający dopuszcza instalację i wdrożenie zdalne przy wykorzystaniu narzędzia Wykonawcy, z zastrzeżeniem, że Wykonawca jest zobowiązany dostarczyć oprogramowanie do zdalnej pracy umożliwiające szyfrowanie połączeń oraz nagrywanie sesji serwisowych.
 - c. W przypadku jeżeli dotyczy, Wykonawca wykona wdrożenie na wybranym serwerze/maszynie wirtualnej wskazanym przez Zamawiającego oraz na stanowiskach wskazanych przez Zamawiającego.
 - d. Wykonawca, pomimo zapewnienia serwisu producenta zobowiązany będzie do udzielania pomocy technicznej Zamawiającemu przez okres gwarancji.
 - e. Usługa wsparcia wdrożenia obejmuje:
 - i. przeprowadzenie analizy przedwdrożeniowej,
 - ii. pomoc przy instalacji silnika bazy danych – jeżeli będzie wymagana instalacja,
 - iii. rejestracja produktu – jeżeli wymagana,
 - iv. instalację oprogramowania: na stacji roboczej lub serwerze – jeżeli dotyczy,
 - v. dystrybucję oprogramowania na wybranych stacjach roboczych – jeżeli dotyczy,
 - vi. konfigurację oprogramowania,
 - vii. optymalizację ustawień pod wymogi sieciowe i sprzętowe Zamawiającego,
 - viii. szkolenie administratorów z zakresu pracy z programem,
 - ix. w uzgodnionym terminie z Zamawiającym zostanie przeprowadzane kontrolne połączenie zdalne w celu weryfikacji ustawień oraz poprawienia konfiguracji.
9. Proces współpracy między Wykonawcą a Zamawiającym w celu wdrożenia oprogramowania – wymagania minimalne:
 - a. Wykonawca przygotowuje projekt techniczny realizacji koncepcji, uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producentów wdrażanego oprogramowania, po wykonaniu analizy istniejącego u Zamawiającego rozwiązania wraz z koncepcją uwzględniające obecne u Zamawiającego uwarunkowania organizacyjne i sprzętowe, łącznie zwane dalej projektem technicznym. W projekcie technicznym muszą być zawarte:
 - i. scenariusze testowe, procedury oraz wzory raportów testów,
 - ii. szczegółowy harmonogram realizacji prac wdrożeniowych i migracyjnych, uwzględniający specyfikę organizacji Zamawiającego,
 - iii. opis koncepcji realizacji prac,
 - iv. zalecenia przedwdrożeniowe dla Zamawiającego, jeżeli będą wymagane.
 - b. Akceptacja projektu technicznego wraz z procedurami oraz wzorami raportów z testów będzie podlegała następującej procedurze:

- i. Wykonawca prześle do akceptacji Zamawiającego, drogą elektroniczną projekt techniczny wraz z procedurami oraz wzorami raportów z testów, w terminie nie dłuższym niż 10 dni roboczych od dnia zawarcia umowy,
 - ii. Zamawiający w terminie nie dłuższym niż 5 dni roboczych od dnia dostarczenia przez Wykonawcę kompletnych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
 - iii. wszystkie uwagi do dokumentów zgłoszone przez Zamawiającego zostaną wprowadzone przez Wykonawcę, w terminie nie dłuższym niż 5 dni roboczych od dnia ich otrzymania,
 - iv. Zamawiający w terminie 5 dni roboczych od dnia powtórnego dostarczenia przez Wykonawcę poprawionych dokumentów, poinformuje Wykonawcę o ich akceptacji lub konieczności wprowadzenia zmian,
 - v. w przypadku nieuwzględnienia uwag Zamawiającego, Zamawiający zastrzega sobie prawo do wskazania ostatecznego terminu dostarczenia projektu technicznego wraz z procedurami oraz wzorami raportów z testów,
 - vi. zatwierdzony projekt techniczny wraz z procedurami zostaną przekazane Zamawiającemu w 1 egzemplarzu oraz w formie elektronicznej na pendrive, w postaci plików do edycji i PDF.
- c. Wykonawca zrealizuje wdrożenia i migracje zgodnie z zakresem prac i projektem technicznym.
 - d. Wykonawca przeprowadzi testy akceptacyjne wdrożonych rozwiązań.
 - e. Wykonawca opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza, w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy. Raport z testów powinien zawierać listę przeprowadzonych testów wraz z ich wynikiem.
 - f. Wykonawca opracuje dokumentację powykonawczą oraz procedury administracyjne i eksploatacyjne w zakresie uzgodnionym z Zamawiającym, w tym: dokumentację wdrożeniową, procedury operacyjne, procedury „Disaster Recovery”. Akceptacja dokumentacji powykonawczej będzie przebiegała zgodnie z zasadami określonymi dla akceptacji projektu technicznego.
10. Wymagania licencyjne dla dostarczonego oprogramowania:
- a. Licencjobiorcą licencji będzie Gmina Rybczewice.
 - b. Zamawiający dopuszcza udzielenie licencji w wersji papierowej i/lub elektronicznej. W przypadku jeżeli producent oprogramowania nie wystawia licencji w zakresie oferowanego oprogramowania Wykonawca powinien dostarczyć stosowne oświadczenie producenta oprogramowania bądź jego dystrybutora.
 - c. Licencje muszą obowiązywać do dnia 30.06.2026 r. niezależnie od modeli dystrybucji poszczególnych producentów oferowanego oprogramowania.
 - d. Oferowane licencje muszą pozwalać na użytkowanie oprogramowania zgodnie z przepisami prawa.
 - e. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do przeniesienia oprogramowania na inny serwer/komputer.

- f. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet). Użytkownik może pracować w dowolny dostępny technologicznie sposób.
 - g. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
 - h. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
 - i. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym urządzeniu klienckim (licencja nie może być przypisana do komputera/urządzenia).
 - j. Licencja oprogramowania nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji ze zgromadzonych danych.
 - k. Wykonawca zapewni gwarancję producenta oprogramowania, która obejmie gwarancję aktualizacji oprogramowania do najnowszej wersji oprogramowania w okresie objętym gwarancją.
11. Wymagania gwarancyjne i serwisowe dla dostarczonego oprogramowania w formie licencji czasowych lub subskrypcyjnych:
- a. Gwarancja producenta musi zostać zapewniona przez Wykonawcę na oferowane oprogramowanie do dnia 30.06.2026 r.
 - b. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w oprogramowaniu do serwisu producenta lub jego dystrybutora.
 - c. Serwis producenta musi zostać zapewniony przez Wykonawcę do dnia 30.06.2026 r.
 - d. Serwis polega na świadczeniu usługi wsparcia technicznego udzielonego przez producenta lub autoryzowanego dystrybutora producenta w języku polskim i objąć musi minimum:
 - i. dostęp do najnowszych wersji oprogramowania,
 - ii. wsparcie telefoniczne w zakresie oferowanego oprogramowania zespołu inżynierów technicznych,
 - iii. wsparcie w prawidłowym i zgodnym z wymaganiami producenta użytkowaniu oprogramowania,
 - iv. przyjmowanie i realizacja zgłoszeń serwisowych,
 - v. doradztwo techniczne w zakresie konfiguracji i optymalizacji oprogramowania,w przypadku jeżeli w dalszej części niniejszego dokumentu zdefiniowano wymogi serwisu lub gwarancji w innym zakresie powyższe wymogi są obowiązujące i należy potraktować jako podstawowe, precyzowane przez dodatkowe wymagania opisane w dalszej części dokumentu.
12. W poniżej wskazanych wymaganiach Zamawiający posługuje się terminami „musi”, „powinien”, „możliwość” określając w ten sposób wymaganą funkcjonalność oprogramowania.

4.2. Zakup oprogramowania do zarządzania infrastrukturą IT (1 szt.).

Przedmiotem zamówienia jest dostawa i wdrożenie oprogramowania w formie licencji wieczystej do zarządzania bezpieczeństwem IT umożliwiającego szereg funkcji podnoszących cyberbezpieczeństwo dla Urzędu Gminy w Rybczewicach.

Wykonawca jest zobligowany wziąć pod uwagę zakres użytkowania oprogramowania obejmujący łącznie maksimum 30 użytkowników/urządzeń.

Minimalne wymagania funkcjonalne dla oprogramowania do zarządzania bezpieczeństwem IT:

1. Funkcjonalność agenta.
 - a) System musi umożliwiać pełne zdalne zarządzanie agentami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączenia agenta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego).
 - b) Agent musi mieć możliwość konfiguracji zakresu skanowania plików.
 - c) Agent musi mieć możliwość wyświetlenia dowolnego komunikatu wysłanego z poziomu konsoli administracyjnej, a konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkownika, który go wyświetlił.
 - d) Agent musi mieć budowę modułową – uniemożliwienie pracy jednego z modułów (np. w wyniku niekompatybilnego systemu operacyjnego, pracy programów firm trzecich, awarii sprzętowej) nie może blokować pracy całego Agent.
2. Funkcjonalność konsoli administracyjnej.
 - a) Konsola musi być w pełni polskojęzyczna.
 - b) Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną.
 - c) Konsola administracyjna musi posiadać dashboardy – dashboard użytkownika, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie.
 - d) Dashboard użytkownika jest budowany samodzielnie przez użytkownika poprzez wybór szybkiego skrótu do dowolnego ekranu aplikacji lub wybór dowolnego widgetu.
 - e) Dashboard prezentujący parametry sieci powinien zawierać widgety pogrupowane w kategorie.
 - f) Konsola administracyjna musi być wyposażona w panel zawierający graficzne widgety prezentujące dane w postaci wykresu kołowego i/lub słupkowego i/lub w formie tabeli z danymi.
 - g) Dane na widgetach muszą być aktualizowane automatycznie lub w każdym czasie na życzenia użytkownika.
 - h) Widgety muszą być skojarzone dziedzinowo ze wszystkimi obszarami zarządzania infrastrukturą.
 - i) System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widgety, ich konfigurację i kolejność).
 - j) Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu. Reguły

muszą być zapamiętywane i dostępne w kolejnych sesjach oraz oparte co najmniej o: nazwę komputera, IP, rodzaj systemu operacyjnego, identyfikator agenta, strukturę organizacyjną, stan agenta (włączony/wyłączony), nazwę użytkownika zalogowanego, producenta sprzętu, dostawcę sprzętu, lokalizację komputera, dowolnie zdefiniowaną przez użytkownika wartość (np. kolor obudowy komputera).

- k) System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, dodawanie, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.
 - l) Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie musi utracić prawa do korzystania z konsoli administracyjnej systemu.
 - m) Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja agenta, stanu agenta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.
 - n) Konsola musi zawierać w sobie pełną dokumentację systemu, dokumentacja musi być na bieżąco aktualizowana poprzez automatyczne mechanizmy aktualizacji z serwera aktualizacji producenta.
3. Zarządzanie licencjami.
- a) System musi umożliwiać zarządzanie licencjami w ramach dowolnego elementu struktury organizacyjnej (dla wybranej struktury organizacyjnej pokazuje liczbę instalacji i liczbę licencji w danym modelu licencjonowania wraz z listą komputerów).
 - b) System musi dawać możliwość wykonywania wielu audytów legalności i zapamiętywać wyniki tych audytów w odniesieniu do systemów operacyjnych jak i aplikacji/pakietów, z uwzględnieniem struktury organizacyjnej.
 - c) System musi pozwalać na zdefiniowanie dowolnej ilości grup oprogramowania.
 - d) System musi umożliwiać zdefiniowanie listy aplikacji zabronionych.
 - e) System musi umożliwiać utworzenie zdefiniowanie oprogramowania zabronionego i w momencie pojawienia się do na komputerze oprogramowanie powinno przystąpić do automatycznego odinstalowania oprogramowania z listy.
 - f) System musi umożliwiać automatyczne przypisanie kategorii do każdego uruchomionego procesu.
 - g) System musi umożliwiać zbieranie szczegółowych informacji o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji).
 - h) System musi umożliwiać odczytywanie identyfikatorów i kluczy produktowych dla systemu operacyjnego.
 - i) System powinien automatycznie klasyfikować licencje OEM dla systemów operacyjnych oraz licencje typu freeware dla aplikacji.
 - j) System musi informować administratora o wygasaniu licencji.
 - k) System musi umożliwiać wyróżnianie licencji zabezpieczonych kluczami sprzętowymi po uprzednim wprowadzeniu numerów licencji.
 - l) System musi automatycznie wskazywać liczbę posiadanych licencji oraz liczbę używanego oprogramowania.

- m) System musi prezentować datę instalacji oprogramowania.
 - n) System musi umożliwiać prowadzenie ewidencji licencji (data zakupu, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT) poprzez rejestrację dokumentów źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium.
 - o) System musi umożliwiać przypisanie licencji do użytkownika i/lub komputera oraz musi udostępniać informację o licencjach zarejestrowanych i nieprzypisanych.
 - p) System musi umożliwiać zbieranie informacji na temat uruchamianych aplikacji na inwentaryzowanych komputerach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji).
 - q) System musi udostępniać informację o uruchamianych aplikacjach w okresie 6 miesięcy oraz udostępniać datę ostatniego uruchomienia.
 - r) System musi umożliwiać podgląd historii zmian aplikacji i pakietów na komputerach.
 - s) System musi umożliwiać zdalne odinstalowanie oprogramowania na wybranych komputerach.
4. Inwentaryzacja sprzętu komputerowego.
- a) System musi umożliwiać automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną.
 - b) System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation).
 - c) System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny, numer części, rozmiar, częstotliwość, taktowanie.
 - d) System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego.
 - e) System musi umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).
 - f) System musi umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).
 - g) System musi umożliwiać skanowanie uprawnień użytkowników oraz grup użytkowników wraz z informacją o uprawnieniach.
 - h) System musi umożliwiać prowadzenie ewidencji zmian konfiguracji sprzętu.
 - i) System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).
 - j) System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium.
5. Inwentaryzacja urządzeń podłączanych do komputera.
- a) System musi automatycznie identyfikować i klasyfikować urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.).
 - b) System musi pozwalać na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.
 - c) System musi ewidencjonować historię podłączanych urządzeń zewnętrznych w zakresie minimum: komputer, data, godzina, użytkownik).
6. Inwentaryzacja urządzeń innych niż komputery.
- a) System musi umożliwiać inwentaryzację manualną (ewidencję) sprzętu innego niż komputery: np. drukarki, switchy, routery, monitory, pamięci masowe itp.

- b) System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner. Skaner musi wykryć typ urządzenia na danym IP/portcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać c najmniej protokół SNMP w wersji 1/2c/3.
 - c) Skaner musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.
 - d) System musi zbierać informacje o prędkości połączenia.
 - e) System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają agenta, a w przypadku, gdy takiego agenta nie posiadają powinien umożliwić zdalną instalację agenta.
 - f) System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci.
 - g) System musi umożliwiać generowanie map według dowolnych filtrów użytkownika.
 - h) System musi monitorować zmiany ewidencyjne i ruchy sprzętu.
 - i) System musi umożliwiać przypisanie urządzenia do użytkownika, ewidencję napraw, gwarancji.
 - j) System musi mieć możliwość przypominania o upływającym terminie gwarancji.
 - k) System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu.
 - l) System musi umożliwiać samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów oraz zapewniać automatyczną numerację tych dokumentów zapewniającą unikatowość.
7. Zdalna administracja komputerami.
- a) System musi automatycznie wykonywać dowolne polecenia na dowolnych komputerach z systemami Windows: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika.
 - b) System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym.
 - c) System musi umożliwiać zdalną instalację poprawek i aktualizacji.
 - d) System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem.
 - e) System powinien być wyposażony w predefiniowane zadania w zakresie minimum: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory windows, włączenie usługi Windows Update, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD).
 - f) Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania oraz udostępniać informację zwrotną o przebiegu wykonania.
 - g) System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, windows powershell.

8. Automatyzacja.

- a) System musi mieć możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące.
- b) Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania danej czynności (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartości parametrów wejściowych, a także zatrzymania/uruchomienia harmonogramu uruchomienia dla każdej z czynności.
- c) System musi mieć możliwość definiowania czynności wykonywanych automatycznie.
- d) System musi być wyposażony w następujące mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów).
- e) System musi być wyposażony w mechanizmy informowania - wysyłania komunikatów (alerty) o: zasobach zakazanych (pliki erotyczne i pornograficzne), zasobach multimedialnych (pliki multimedialne), nowych komputerach w bazie danych, braku skanowania komputerów, brakach w licencjach, niewłaściwych danych systemowych komputerów, urządzeniach bez użytkowników, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, wygasaniu serwisu lub licencji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, upływającej gwarancji,
- f) System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).
- g) System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)
- h) System musi umożliwiać tworzenie zadań cyklicznych dla komputerów.

9. Repozytorium.

- a) Konsola administracyjna musi być wyposażona w repozytorium dokumentów dowolnego typu.
- b) Repozytorium musi umożliwiać: dodawanie nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium w dowolnym miejscu systemu, uzyskanie informacji w jakich miejscach systemu dany dokument repozytorium występuje.

10. Monitorowanie drukarek sieciowych i wydruków.

- a) System musi posiadać możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa).
- b) Ewidencja wydruków musi obejmować minimum: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera, z którego dokonano wydruku, format dokumentu, informację o jednym bądź dwustronnym wydruku, informację o wydruku mono/kolor.
- c) System musi generować zestawienia pozwalające ustalić miejsca powstawania wydruków (komórki organizacyjne, użytkownicy) oraz stopień obciążenia poszczególnych urządzeń drukujących.
- d) Dla każdej z drukarek SNMP system musi udostępniać informacje: nr seryjny, IP, MAC, bieżący status drukarki, całkowitą ilość wydrukowanych stron, ilość wydrukowanych stron od uruchomienia, błędy, alerty, dostępne porty, stan pokryw, interfejsów sieciowych, rodzaj i ilości pamięci całkowitej i wykorzystanej, informacje o poziomie materiałów eksploatacyjnych

11. Monitorowanie stron www.

- a) System musi posiadać możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej.
- b) Ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek.
- c) Ewidencja otwieranych stron musi działać również, gdy otwierana jest strona z połączeniem szyfrowanym (https).
- d) Ewidencja musi obejmować co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony, łączny czas korzystania, czas aktywności, czas pasywności.

12. Monitorowanie dziennika zdarzeń.

- a) System musi posiadać możliwość monitorowania dziennika zdarzeń wszystkich komputerów.
- b) Ewidencja zdarzeń musi następować w oparciu o definiowalną kategorię zdarzenia: critical, error, warning, info, debug oraz typ dziennika: aplikacja, bezpieczeństwo, system.
- c) System musi pozwalać na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia.
- d) Ewidencja musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia.
- e) System musi umożliwiać monitorowanie komunikatów Syslog.

13. Monitorowanie pracy komputerów.

- a) System musi posiadać możliwość monitorowania daty włączenia i wyłączenia komputera niezależnie czy znajduje się w sieci lokalnej czy też poza nią i prezentować czas pracy komputera w układzie graficznym.
- b) System musi posiadać ewidencję daty i godziny przyłączenia i odłączenia komputera od systemu monitorującego.
- c) System musi ewidencjonować zdarzenia związane z logowaniem się użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie

14. Monitorowanie sesji zdalnych połączeń.

- d) System musi prowadzić ewidencję sesji zdalnych połączeń na każdym komputerze.
- e) Informacja o nawiązanej sesji musi zawierać co najmniej: nazwę i adres IP komputera, z którego nastąpiło połączenia, nazwę użytkownika nawiązującego połączenie.

15. Raportowanie i eksport danych.

- a) System musi mieć możliwość kategoryzowania raportów (spośród wszystkich raportów) oraz dodawania raportów użytkownika (zaprojektowanych przez użytkownika).
- b) System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów.
- c) System musi umożliwiać eksport danych z raportu do formatów: PDF, XLS.
- d) System musi posiadać grupę zdefiniowanych raportów dotyczących wszystkich obszarów funkcjonalnych.
- e) System musi posiadać możliwość ustalenia harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu.

16. Powiadomienia.

- a) System musi umożliwiać generowanie powiadomienia w formie alertu w konsoli systemu, wiadomości email wysłanej na wybrane adresy oraz wiadomości SMS na wskazane numery telefonów.
- b) System musi umożliwiać tworzenie wybranych powiadomień wiele razy z określeniem innych grup obiorców.

- c) System musi umożliwiać edycję treści wysyłanych powiadomień i możliwość korzystania z danych umieszczonych w systemie w treści powiadomienia.
- d) System musi posiadać grupę zdefiniowanych powiadomień dotyczących obszarów funkcjonalnych.

17. Bezpieczeństwo.

- a) System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.
- b) Uwierzytelnianie do systemu musi być realizowane z wykorzystaniem imiennego konta użytkownika i hasła, z wykorzystaniem imiennego konta administratorów aplikacji i hasła, za pośrednictwem jednokrotnego uwierzytelniania poprzez Active Directory.
- c) Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej.
- d) Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków.
- e) System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie.
- f) System musi udostępniać historię korzystania z poszczególnych opcji przez wybranych użytkowników/administratorów.
- g) System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nieprzyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.
- h) System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od agentów.

18. Monitorowanie czasu pracy.

- a) System musi mieć możliwość zdefiniowania dowolnej ilości reguł dotyczących czasu pracy komputera.
- b) System musi mieć możliwość zdefiniowania zalecanego czasu pracy dla każdego komputera, przy czym czas pracy w każdym dniu tygodnia może być zdefiniowany inaczej.
- c) System musi mieć możliwość automatycznego dołączenia bieżącego zrzutu ekranu do każdego incydentu związanego z przekroczeniem zalecanego czasu pracy.

19. Zarządzanie politykami bezpieczeństwa.

- a) System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji.
- b) System musi mieć możliwość definiowania obiektów, na których działać będzie reguła w oparciu o parametry: nazwę komputera, adres IP, unikatowy identyfikator agenta, nazwę systemu operacyjnego, zalogowanego użytkownika, model komputera, strukturę organizacyjną, producenta komputera, dostawcę komputera, budżet z jakiego komputer został zakupiony.
- c) Nowy komputer zgłaszający się do systemu po raz pierwszy musi bez dodatkowej ingerencji administratora automatycznie pobrać oraz wdrożyć (uruchomić) przeznaczoną dla niego politykę.
- d) System musi mieć możliwość określenia ram czasowych działania danej reguły

4.3. Rozbudowa oprogramowania antywirusowego o funkcje EDR (1 szt.).

Aktualnie Zamawiający posiada licencję oprogramowania antywirusowego Bitdefender Endpoint Security Tool. Przedmiotem zamówienia jest rozbudowa oprogramowania do wersji Bitdefender GravityZone Business Security Enterprise (Ultra z EDR) wraz z modułem do szyfrowaniem dysków i zarządzaniem podatnościami w okresie do dnia 30.12.2026 r. obejmująca maksymalnie 30 użytkowników indywidualnych oraz 3 urządzenia serwerowe lub dostawa równoważnej platformy bezpieczeństwa zgodnie z funkcjonalnymi kryteriami równoważności określonymi poniżej.

Minimalne wymagania (kryteria równoważności) określone dla równoważnej platformy bezpieczeństwa:

Ochrona antywirusowa i antyspyware:

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Interfejs oraz pomoc techniczna świadczona w języku polskim.
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi.
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
5. Wbudowana technologia do ochrony przed rootkitami.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. Możliwość ustawienia zadania skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Ochrona krytycznych kluczy rejestru przed ich wykorzystaniem lub nieautoryzowanym dostępem do nich.
13. Możliwość dodawania wykluczeń na podstawie:
 - a. Plik
 - b. Folder
 - c. Rozszerzenie
 - d. Proces
 - e. Hash pliku
 - f. Hash certyfikatu
 - g. Nazwa zagrożenia
 - h. Wiersz poleceń
 - i. IP/maska
14. Skanowanie poczty opartej o protokoły POP3 i SMTP w czasie rzeczywistym.
15. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie w przeglądarce.

16. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
17. Wsparcie przeglądarek Internet Explorer 8+, Mozilla Firefox 30+, Google Chrome 34+, Safari 4+, Microsoft Edge 20+ i Opera 21+ bez konieczności zmian w konfiguracji.
18. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH.
19. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
20. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
21. W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i godziny.
22. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
23. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
24. Administrator musi mieć możliwość ukrycia ikony oprogramowania w obszarze powiadomień systemu Windows.
25. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na punkcie końcowym Windows i macOS.
26. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
27. Oprogramowanie klienckie posiada wbudowaną funkcję do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
28. System musi umożliwiać kontrolę dostępu do urządzeń na podstawie interfejsów, do których zostały one podłączone.
29. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej na podstawie ich wykrycia lub wpisanych ręcznie ID urządzenia lub ID produktu.
30. Funkcja blokowania informacji wysyłanych przez HTTP lub SMTP jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.).
31. Funkcja blokowania wysyłanych informacji konfigurowana zdalnie przez administratora.
32. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
33. Wbudowany IDS.
34. Możliwość wykorzystania funkcji skanowania lokalnego lub hybrydowego ze sprawdzaniem reputacji plików w chmurze.
35. Możliwość tworzenia list sieci zaufanych.
36. Możliwość dezaktywacji funkcji zapory sieciowej.
37. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
38. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa).
39. Komunikacja między konsolą zarządzającą, a punktami końcowymi jest szyfrowana.
40. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:
 - a. Możliwość wymuszenia funkcji DEP systemu Windows.

- b. Możliwość wymuszenia relokacji modułów (ASLR) dla Windows.
41. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci.
 42. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików w momencie szyfrowania, a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.
 43. System musi wykrywać podatne sterowniki zainstalowane na punkcie końcowym z Windows i Linux.
 44. Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności w systemie Windows.
 45. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows.
 46. System musi umożliwiać skanowanie oprogramowania układowego UEFI.
 47. System umożliwia przechwytywanie TLS handshake pozwalając na skanowanie ruchu sieciowego bez konieczności deszyfracji.
 48. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows i macOS do SIEM Splunk (wymaga TLS 1.2 lub wyższy) lub z systemem Windows i Linux do serwera Syslog (JSON).
 49. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników naruszeń bezpieczeństwa (IOC).

Stacje robocze i serwery.

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
4. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
5. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
6. Produkt i zawartość zabezpieczeń powinny być aktualizowane nie rzadziej niż raz na godzinę.
7. Oprogramowanie posiada możliwość raportowania zdarzeń informacyjnych.
8. Oprogramowanie musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
9. Oprogramowanie musi posiadać możliwość skanowania jedynie nowych i zmienionych plików.
10. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji na systemach Windows po doinstalowaniu odpowiedniego modułu. Zmiana ustawień zabezpieczona jest hasłem.
11. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji „O programie”, możliwość wyświetlenia danych do pomocy technicznej tj: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony z wyłączeniem systemów Linux.

12. Dla maszyn z systemem Linux możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym.

Ochrona Exchange.

1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w ciągu określonego czasu.
3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz niemożliwych do przeskanowania.
4. Możliwość skanowania w poszukiwaniu potencjalnie niechcianych aplikacji (PUA).
5. Możliwość skanowania malware wewnątrz archiwów.
6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.
7. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.
8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy.
9. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi.
10. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowanie maila do konkretnej skrzynki pocztowej.
11. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.
12. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.

Konsola zdalnej administracji.

1. System musi umożliwiać centralne zarządzanie i konfigurację ochrony wspieranych stacji roboczych i serwerów.
2. Możliwość integracji wielu domen Active Directory.
3. Możliwość uruchomienia zdalnego skanowania wybranych punktów końcowych.
4. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony punktu końcowego (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania na żądanie, zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
5. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi.
6. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, systemu operacyjnego.

7. Możliwość centralnej aktualizacji punktów końcowych z serwera w sieci lokalnej lub z Internetu.
8. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
9. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
10. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) oraz wyeksportowanie ich do formatu: pdf i csv. Również zbiorczo w formie archiwum zip.
11. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie.
12. Możliwość generowania raportu co godzinę.
13. Pierwsza aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
14. Możliwość dodania etykiety do stacji roboczej.
15. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
16. Możliwość przechowywania kwarantanny maksymalnie 180 dni.
17. Możliwość definiowania, czy pliki z kwarantanny mają być przesyłane do producenta i co ile godzin ma się ta czynność odbywać.
18. Po aktualizacji zawartości bezpieczeństwa opcja automatycznego przeskanowania kwarantanny.
19. Wsparcie techniczne mailowe i telefoniczne w j. polskim od poniedziałku do piątku w godzinach 8:00-16:00. W pozostałych godzinach możliwość bezpośredniego kontaktu z producentem (24/7) w j. angielskim.
20. Po integracji z lokalnym Active Directory możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
21. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238.
22. Możliwość naprawy instalacji agenta z poziomu konsoli.
23. Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej, jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn, które automatycznie będą usuwane oraz na określenie godziny, o której te maszyny będą usuwane.
24. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
25. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
26. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux lub MacOS.
27. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
28. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS.
29. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M oraz osobnego pakietu dla systemów Windows z Intel x86 oraz oddzielnego dla architektury ARM.
30. System umożliwia pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli administracyjnej.
31. Możliwość wygenerowania i zapisania logów na stacji roboczej z poziomu konsoli zarządzającej.
32. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.

33. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Przypisywanie musi odbywać się ręcznie lub automatycznie. Musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
34. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego.
35. Wbudowany sandbox musi działać w trybie monitorowania i blokowania.
36. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja, przeniesienie do kwarantanny lub tylko raportowanie.
37. Wbudowany sandbox musi oferować opcję wstępnego filtrowania plików z kategorii aplikacje, dokumenty, skrypty, archiwa, maile zapisane do pliku, pod kątem podejrzanego zachowania.
38. Wbudowany sandbox musi posiadać opcję, która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.
39. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.
40. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.
41. Możliwość zablokowania konta w konsoli, jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.
42. Funkcja pojedynczego logowania – Single Sign-on (SSO) przy integracji z Microsoft Azure.
43. Oprogramowanie musi umożliwiać tworzenie konfigurowalnych reguł, po spełnieniu których może zostać wygenerowany incydent bezpieczeństwa.

EDR-Endpoint Detection and Response.

1. Moduł musi umożliwiać monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności.
2. Moduł musi bazować na systemach opartych o techniki MITRE ATT&CK i własnej inteligencji.
3. Moduł musi umożliwiać zgłaszanie naruszeń jako incydent w module EDR.
4. Moduł musi umożliwiać wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym czasie.
5. Moduł musi umożliwiać integrację się z bazą wiedzy MITRE ATT&CK i odpowiednio oznaczać zdarzenia bezpieczeństwa.
6. Moduł musi umożliwiać wizualizację zdarzeń bezpieczeństwa z określonymi danymi lub działaniami z następującymi informacjami:
 - a. Karta podsumowująca zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia.
 - b. Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej.
 - c. System gromadzi informacje o działaniach podejmowanych przez produkt w związku ze zdarzeniem bezpieczeństwa.
7. Moduł musi umożliwiać informowanie o zagrożeniach wykrytych i zablokowanych w formie graficznej i chronologicznej linii zdarzeń w zakresie minimum:
 - a. Filtrowania zdarzeń.

- b. Zakończenia procesów.
 - c. Dodania procesów do czarnej listy.
 - d. Dodania procesów do białej listy.
 - e. Izolacji hosta.
 - f. Przesłania pliku do Sandbox.
 - g. Sprawdzenia informacji o pliku w Google.
 - h. Sprawdzenia informacji o pliku w VirusTotal.
8. Moduł musi umożliwiać podgląd incydentów za pomocą spersonalizowanych widoków list lub widoku domyślnego.
 9. Moduł musi umożliwiać blokowanie na podstawie utworzonych reguł czarnej listy przy pomocy kategorii:
 - a. Hash MD5 lub SHA256.
 - b. Pełna ścieżka do aplikacji.
 - c. Reguła połączenia.
 10. Moduł musi umożliwiać import reguł czarnej listy dla hash, ścieżek do aplikacji oraz reguł połączeń z pliku CSV.
 11. Moduł musi oferować zakres filtrowania dodanych reguł blokowania minimum po nazwie pliku, hash pliku, typu hash, ścieżce, protokole porcie/zakresie portów, daty dodania.

Pełne szyfrowanie dysków (FDE- Full Disk Encryption).

1. Moduł może wykorzystywać natywną funkcję BitLocker na systemach Windows oraz funkcję FileVault na systemach macOS.
2. Moduł musi umożliwiać szyfrowanie i deszyfrowanie punktów końcowych poprzez politykę bezpieczeństwa zastosowaną na komputerach.
3. Moduł musi umożliwiać podgląd klucza odzyskiwania do funkcji Bitlocker z konsoli administracyjnej po wpisaniu hasła.
4. Moduł musi umożliwiać ustawienie PIN do funkcji szyfrowania.
5. Moduł musi zapewniać zgodność z wymogami RODO odnośnie do szyfrowania danych.
6. Administrator modułu musi mieć możliwość ustawienia, czy system szyfrujący ma pytać o hasło w momencie uruchomienia systemu operacyjnego, jeśli aktywny jest moduł TPM.
7. Moduł musi automatycznie importować klucz odzyskiwania do konsoli po instalacji oprogramowania z modułem szyfrowania.
8. Moduł musi mieć możliwość dodania wyjątków od szyfrowania dla dysków innych niż systemowe.

4.4. Zakup oprogramowania backup (1 szt.).

Minimalne parametry funkcjonalne oprogramowania:

1. Wymagania ogólne:
 - a) licencja wieczysta na oprogramowanie ma umożliwiać backup 15 środowisk;
 - b) oprogramowanie musi współpracować z infrastrukturą VMware oraz Microsoft Hyper-V;
 - c) oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami;

- d) oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami;
- e) oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V;
- f) oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux;

2. Całkowite koszty posiadania:

- a) oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej;
- b) oprogramowanie musi tworzyć „samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków;
- c) oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy;
- d) oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów;
- e) oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli;
- f) oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu;
- g) oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota;
- h) oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API;
- i) oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji;
- j) oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej;
- k) oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji konsol administracyjnych.

3. Wymagania RPO:

- a) oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji;
- b) oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty, które mogą zakłócić poprawne wykonanie backupu bez konieczności interakcji administratora;
- c) oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych;
- d) oprogramowanie musi posiadać wsparcie dla VMware vSAN;

- e) oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn;
- f) oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN;
- g) oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

4. Wymagania RTO:

- a) oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
- b) dodatkowo dla środowiska vSphere powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna);
- c) oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny;
- d) oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere;
- e) oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków;
- f) oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny;
- g) oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej;
- h) oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.

5. Monitoring:

- i) system musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich;
- j) system musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn;
- k) system musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej;
- l) system musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora;
- m) system musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej;
- n) system musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego;

- o) system musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

6. Raportowanie:

- a) system raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej;
- b) system musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc;
- c) system musi mieć możliwość ustawienia harmonogramu generowania raportów;
- d) system musi mieć możliwość generowania raportów z dowolnego punktu w czasie;
- e) system musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.