Załącznik nr 1.1. do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA- Zadanie 1

Strony zgodnie stwierdzają, że na potrzeby niniejszego OPZ wraz z załącznikami i przyszłej Umowy dotyczącej opisanego zamówienia, wymienionym w niniejszym paragrafie pojęciom nadają znaczenie określone poniżej, oraz że użyte w tekście poniżej wymienione pojęcia, rozumiane będą w sposób poniżej zdefiniowany. Dla podkreślenia, że pojęcia te rozumiane są w sposób zdefiniowany, ich pierwsze litery będą pisane w tekście wielką literą.
Strony ustalają następujące definicje:

1. **Zamawiający** – oznacza podmiot który udziela zamówienia – Zespół Opieki Zdrowotnej „Spitala Powiatowego" w Sochaczewie
2. **Wykonawca** - podmiot, który ubiega się o udzielenie zamówienia, złożył ofertę albo zawarł umowę w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez prowadzenia negocjacji na podstawie art. 275 pkt 1 Ustawy z dnia 11 września 2019r – prawo zamówień publicznych (Dz.U. poz. 2019 ze zm.).
3. **Strony** - podmioty bezpośrednio uczestniczące w umowie zawiązanej na podstawie rozstrzygnięcia podstępowania przetargowego.
4. **System informatyczny** - zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej. W skład systemu wchodzą najczęściej elementy: Sprzęt komputerowy, Oprogramowanie narzędziowe, Oprogramowanie dziedzinowe.
5. **Infrastruktura sprzętowa -** znajdująca się w dyspozycji Zamawiającego, w tym stanowiąca jego własność oraz dostarczana w ramach realizacji przedmiotu zamówienia infrastruktura przetwarzania danych wszystkie połączenia, urządzenia fizyczne i oprogramowania aplikacyjne, które łącznie współpracując umożliwiają gromadzenie, przechowywanie, wytwarzanie danych i usług oraz udostępnianie danych i usług elektronicznych.
6. **Umowa** – umowa zawarta w ramach realizacji OPZ.
7. **SWZ –** Specyfikacja Warunków Zamówienia
8. **Gwarancja i Serwis Oprogramowania** – Oznacza całokształt świadczonych przez Wykonawcę usług (gwarancyjno-serwisowych) związanych z zapewnieniem poprawnej pracy składników będących przedmiotem zamówienia, szczegółowo określone w niniejszym dokumencie w oraz w projekcie umowy.
9. **Gwarancja i Serwis Infrastruktury Sprzętowej** – Oznacza całokształt świadczonych przez Wykonawcę usług (gwarancyjno-serwisowych) związanych z zapewnieniem poprawnej pracy składników będących przedmiotem zamówienia, szczegółowo określone w niniejszym dokumencie oraz w projekcie umowy.
10. **Sprzęt Komputerowy** – zestaw komputerów (w tym stacje robocze, sprzęt serwerowy, terminale) i oprzyrządowania, na którym pracuje oprogramowanie.
11. **System Komunikacyjny** – infrastruktura telekomunikacyjna, sieciowa, systemy separacji, systemy bezpieczeństwa oraz certyfikaty serwerów WWW, obejmujące elementy lokalnej sieci komputerowej, łącza i urządzenia rozległej sieci transmisji danych oraz urządzenia komutacji pakietów wraz z ich oprogramowaniem, odpowiedzialne za obsługę HIS.
12. **Oprogramowanie Narzędziowe** – elementy oprogramowania zainstalowane na Sprzęcie Komputerowym, obejmujące w szczególności:
    - systemy operacyjne (np. Windows, LINUX, UNIX),
    - system zarządzania bazą danych (SZBD), zwane też oprogramowaniem bazodanowym (np. MSSQL, Oracle),
    - oprogramowanie służące do administracji i zarządzania Sprzętem Komputerowym, systemem operacyjnym i systemem zarządzania bazą danych,
    - oprogramowanie komunikacyjne umożliwiające podłączenie stacji dostępowych do serwera bazy;
13. **Plan Realizacji Projektu** – Dokument określający zasady współpracy pomiędzy Zamawiającym, a Wykonawcą. Zawiera m.in.:
    - strukturę organizacyjną projektu,
    - produkty projektu,
    - zasady komunikacji w projekcie,
14. **Szkolenie Administratora(ów)** – szkolenia użytkownika(ów) wskazanych przez Zamawiającego do pełnienia funkcji administratora infrastruktury sprzętowej.
15. **Systemy Zewnętrzne** – systemy z którymi docelowo współpracować będzie wdrażany system.

16. **Wdrożenie** – etap cyklu życia systemu informatycznego, polegający na instalacji i dostosowaniu oprogramowania do wymagań Zamawiającego oraz testowaniu i uruchomieniu systemu informatycznego.
    - Podstawowe etapy procesu wdrożenia:
    - Przygotowanie dokumentacji,
    - Przygotowanie i skonfigurowanie infrastruktury technicznej,
    - Zainstalowanie i skonfigurowanie systemu informatycznego do eksploatacji,
    - Testowanie systemu,
    - Uruchomienie produkcyjne systemu.
17. **Środowisko Zapasowe** – kopia Środowiska Produkcyjnego lub jego części, służąca do gromadzenia kopii rzeczywistych danych biznesowych Zamawiającego i podjęcia ich przetwarzania w przypadku awarii Środowiska Produkcyjnego lub w celach przeprowadzenia testów wdrożeniowych aktualizacji/nowych funkcjonalności.
18. **Zdalny Dostęp** – analogowe lub cyfrowe łącze wydajnej transmisji danych pomiędzy węzłem infrastruktury siedziby Wykonawcy, a węzłem infrastruktury zapewnianym przez Zamawiającego, umożliwiające realizować usługi serwisowe lub konfiguracyjne.
19. **Szczegółowym Harmonogramem Realizacji Zadania** – szczegółowy terminarz realizacji przedmiotu Umowy wraz z podziałem na Etapy przygotowany przez Wykonawcę w terminie 14 dni roboczych od zawarcia umowy.
20. **Zadanie** – przedmiot zamówienia (przedmiot Umowy) wynikający łącznie z SWZ, Oferty Wykonawcy, Umowy.
21. **Etap** – główny element części Zadania, stanowiący funkcjonalną całość, podlegająca odrębnym odbiorom. Każdy Etap stanowi odrębną część (rozdział) niniejszego OPZ.
22. **Protokół Odbiorczy** – protokół przygotowany przez Wykonawcę, będący potwierdzeniem przyjęcia przez Zamawiającego wykonanych przez Wykonawcę prac będących przedmiotem poszczególnych Etapów.
23. **Protokół Uzgodnień** – dokument tworzony przez Wykonawcę i zatwierdzony przez Strony, na podstawie zapisu ze spotkania lub ustaleń zdalnych (mailowych, telefonicznych) z Zamawiającym. Dokument ten używany jest w trakcie prowadzenia analizy wymagań Zamawiającego i stanowi zobowiązanie obu Stron. Zamawiający zobowiązany jest, że wymagania zapisane w/w protokole nie zostaną zmienione, natomiast Wykonawca zobowiązany jest do realizacji zawartych w nim wymagań Zamawiającego. W przypadku zajścia konieczności wykonania zmian lub innych czynności niż te, które zostały opisane w Protokole Uzgodnień, należy utworzyć nowy Protokół Uzgodnień zawierający te zmiany. W Protokole Uzgodnień można zamieścić inne uzgodnienia, niezwiązane z wymaganiami projektu, tj. ustalenia organizacyjne.
24. **Dzień Roboczy** – każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
25. **Godziny Robocze** – godziny od 7:30 do 14:30 w każdym Dniu Roboczym.
26. **Kierownik Zamawiającego** – osoba wyznaczona przez Zamawiającego, koordynująca całość przedmiotu danego pakietu, posiadająca odpowiednie pełnomocnictwa. W szczególności odpowiedzialna ze strony Zamawiającego za realizację przedmiotu zamówienia.
27. **Kierownik Wykonawcy** - osoba wyznaczona przez Wykonawcę do koordynacji realizacji prac danego zadania. Upoważniona do podpisywania Dokumentacji Projektu z ramienia Wykonawcy.
28. **Elektroniczny System Zgłoszeń (ESZ)** – narzędzie posiadające interfejs WWW służące do rejestracji zgłoszeń (potencjalnych problemów, usterek) oraz kontroli ich cyklu życia (tzw. Issue Tracking System lub Defect Tracking System). System ESZ udostępniony zostanie przez Wykonawcę dla Zamawiającego na czas realizacji przedmiotu zamówienia oraz w okresie jego gwarancji.

OPIS RÓWNOWAŻNOŚCI:

W przypadku gdy w dokumencie stanowiącym element opisu przedmiotu zamówienia pojawią się wskazania znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego dostawcę (jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub jego produktów), należy rozumieć, zgodnie z przepisem art. 99 ust. 5 ustawy Pzp, że zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób i w takich okolicznościach Zamawiający dopuszcza możliwość składania w ofercie rozwiązań równoważnych, wskazując, iż minimalne wymagania, jakim mają odpowiadać rozwiązania równoważne, to wymagania nie gorsze od parametrów wskazanych w tych dokumentach, a ich kryteria w celu oceny równoważności wskazane są w opisie przedmiotu zamówienia.

W przypadku, gdy Zamawiający opisuje przedmiot zamówienia przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy, zamawiający dopuszcza rozwiązania równoważne opisywanym.
Wykonawcy mogą składać oferty zawierające rozwiązania równoważne w stosunku do przedmiotu zamówienia przedstawionego w SWZ – zgodnie z art. 101 ust. 4, 5 i 6 ustawy PZP, jednak są zobowiązani wykazać, że oferowane przez nich rozwiązania spełniają wymagania określone przez Zamawiającego. Równoważność pod względem parametrów technicznych, użytkowych oraz eksploatacyjnych ma w szczególności zapewnić uzyskanie parametrów nie gorszych od założonych w niniejszym SWZ
Za równoważne uznaje się rozwiązania, jak również elementy, materiały, urządzenia o właściwościach funkcjonalnych i jakościowych takich samych, które zostały określone w opisie przedmiotu zamówienia, lecz oznaczonych innym znakiem towarowym, patentem lub pochodzeniem. Przy czym istotne jest to, że produkt równoważny to produkt, który nie jest identyczny, tożsamy z produktem referencyjnym, ale posiada pewne, istotne dla Zamawiającego, zbliżone do produktu referencyjnego cechy i parametry.
Istotne dla Zamawiającego cechy i parametry, to takie, które pozwolą zachować wszystkim systemom, urządzeniom, wyrobom, parametry i cechy pozwalające przede wszystkim na prawidłową współpracę z innymi systemami i/lub urządzeniami i/lub wyrobami w sposób założony przez Zamawiającego oraz pozwalające przy tym uzyskać parametry nie gorsze od założonych w niniejszym załączniku. Ciężar udowodnienia równoważności spoczywa na Wykonawcy

Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowany przedmiot zamówienia spełnia wymagania określone przez Zamawiającego poprzez złożenie opisu zaoferowanych produktów wraz z wykazaniem cech równoważności w stosunku do wymagań opisanych przez Zamawiającego w niniejszym załączniku oraz podanie nazwy handlowej i producenta.

W celu wykazania cech równoważności Zamawiający dopuszcza załączenie do opisu etykiet, zdjęć, kart katalogowych itp., z dopiskiem której pozycji asortymentowej (jakiego sprzętu) dotyczy dana informacja z zastrzeżeniem, że z tych dokumentów muszą wynikać parametry co najmniej określone przez Zamawiającego w załącznikach do OPZ i dane identyfikujące produkt.

DOSTAWA INFRASTRUKTURY SPRZĘTOWEJ ORAZ OPROGRAMOWANIA

Przedmiotem zamówienia jest dostawa sprzętu i oprogramowania podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych w Zespole Opieki Zdrowotnej Szpitala Powiatowego w Sochaczewie.
Poniżej wyspecyfikowano minimalne parametry sprzętu oraz oprogramowania, które należy dostarczyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.
Wymagania ogólne:

- Całość dostarczanego sprzętu i oprogramowania standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
- Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, musi być nowe, wcześniej nieużywane, rok produkcji nie starszy niż 2021.
- Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, w którym nie wskazano szczegółowych warunków gwarancji, musi być objęte minimum 12 miesięczną gwarancją jeśli w opisie parametrów nie wskazano inaczej
- Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
- Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
- Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
- Wszystkie urządzenia muszą posiadać oznakowanie CE.
- Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
- Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
- Wymagane jest, aby infrastruktura sprzętowa była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
- Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).
- Wykonawca w celu zabezpieczenia danych krytycznych przetwarzanych w systemie HIS Zamawiającego zobowiązany jest dołączyć do oferty potwierdzenie, że posiada uprawnienia lub autoryzację producenta

systemu medycznego, z którego obecnie korzysta Zamawiający lub zrealizował przedmiot zamówienia w obszarze dotyczącym ingerencji w dane przetwarzane przez system medyczny Zamawiającego nie naruszając postanowień licencyjnych i gwarancyjnych dla systemu medycznego i gwarantował jego poprawne monitorowanie po zakończeniu prac integracyjnych.
Powyższe zobowiązanie wynika z konieczności monitoringu krytyczne elementy systemu HIS w ramach dostawy Systemu monitoringu infrastruktury IT.
Zamawiający wymaga aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:

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

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

1. Wykonanie Projektu Technicznego dostarczanej infrastruktury sprzętowej, który będzie składał się co najmniej z następujących elementów:
   - Dokładna specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów,
   - Nazwy oraz szczegółowa adresacja poszczególnych elementów,
   - Planowana konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsca, zaprojektowanie kompleksowego systemu ochrony danych opartego na funkcjach macierzy oraz oprogramowania standardowego z uwzględnieniem specyfiki całego projektu,
   - Wymagane działania ze strony Zamawiającego w celu poprawnego montażu i konfiguracji,
   - Harmonogram prac.

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

Opis parametrów minimalnych dostarczanej infrastruktury oraz oprogramowania:
Wymagania dla Wykonawcy który dostarczy infrastrukturę sprzętową oraz oprogramowanie:
Zamawiający wymaga, aby Wykonawca spełniała wymagania w zakresie:

1. System monitoringu infrastruktury IT (SOC) – usługa świadczona od dnia podpisania umowy do 31.12.2022

Lp.	Wymagane minimalne parametry techniczne	Wymóg do spełnienia (warunek graniczny)	OFEROWANE PARAMETRY TECHNICZNE - podaje Wykonawca Wymogi dotyczące opisu oferowanych parametrów: TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę NIE – wykonawca nie spełnia konkretnego parametru
Użytkownicy			
1.	▪ Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat. ▪ Zapewnienia równoległego dostępu do systemu dla wielu użytkowników. ▪ Ograniczania użytkownikom dostępu do wybranych grup hostów.	TAK	
Monitorowanie			
1.	▪ Monitorowania serwerów fizycznych. ▪ Monitorowania urządzeń sieciowych. ▪ Monitorowania stanu połączeń. ▪ Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów ▪ Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux. ▪ Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych. ▪ Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń. ▪ Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu. ▪ Grupowanie hostów. ▪ Definiowanie planowanych przerw serwisowych dla hostów i usług. ▪ Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK). ▪ Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień; konfiguracje przerw serwisowych). ▪ Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www). ▪ Monitorowanie serwerów za pomocą agentów ▪ Monitorowanie serwerów aplikacji: Tomcat, Oracle WebLogic Server, Oracle Application Server . ▪ Monitorowanie Active Directory. ▪ Monitorowanie serwerów plików, udziałów sieciowych. ▪ Monitorowanie statusu serwerów Apache. ▪ Monitorowanie baz danych: – ORACLE, – MySQL,	TAK	

	– Postgress. – MSSQL Server – DB2 ▪ Monitorowanie urządzeń przez następujące protokoły: – SNMP, – WMI, – IPMI. ▪ Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW. ▪ Monitorowanie poprawności działania DNS. ▪ Monitorowanie środowiska VMware. ▪ Monitorowanie środowiska Hyper-V. ▪ Monitorowanie działania serwera czasu NTP. ▪ Monitorowanie offsetu czasu na serwerach. ▪ Monitorowanie ping - czasy odpowiedzi, straty pakietów. ▪ Monitorowanie zajętości miejsca na poszczególnych partycjach. ▪ Monitorowanie obciążenia dysków. ▪ Monitorowanie wykorzystania pamięci RAM. ▪ Monitorowanie obciążenia CPU. ▪ Monitorowanie logów systemowych Windows. ▪ Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia. ▪ Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane. ▪ Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Linux i Unix. ▪ Agregację usług niskiego poziomu do procesów biznesowych (tzw. Business Intelligence) ▪ Symulację awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe ▪ Monitorowanie rozproszone (podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji/oddziałów). ▪ Wykrywanie niestabilnie działających usług. ▪ Monitorowanie dostępności stron internetowych. ▪ Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządzeń).		
Prezentacja			
1.	▪ Prezentację stanu urządzeń na mapie. ▪ Prezentację danych na dashboardach. ▪ Elastyczną konfigurację dashboardów, wybór elementów. ▪ Wizualizację stanu działania całej infrastruktury na jednym dashboardzie. ▪ Tworzenie indywidualnych dashboardów przez użytkowników	TAK	

Powiadomienia			
1.	▪ Globalne wyłączanie powiadomień. ▪ Powiadamianie użytkownika o problemach przez e-mail. ▪ Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie. ▪ Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do poszczególnych użytkowników. ▪ Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług	TAK	
Konfiguracja			
1.	▪ Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW ▪ Automatyczna konfiguracja i działanie z REST-API ▪ Centralne zarządzanie agentami ▪ Integracja danych z różnych źródeł danych (JSON, XML, SNMP)	TAK	
Monitoring bazy danych systemu HIS			
1.	Możliwość monitorowania bazy danych systemu HIS w zakresie co najmniej: – Instance state – Version – Jobs – Locks – Processes – Number of active sessions – Recovery area – Log switch activity – General tablespace information – Tablespaces performance – Long active sessions – Undo retention – Checkpoint and online backup state – Custom SQLs – RMAN backup status – RMAN backups – ASM disk groups – Apply and transport lag of Oracle Data-Guard – Możliwość dodania własnych zapytań SQL i monitorowanie zwracanych wartości	TAK	
Kolektor logów			
1.	▪ System posiada własny kolektor logów syslog ▪ Może odbierać wiadomości bezpośrednio z syslog lub SNMP traps ▪ Za pomocą agentów potrafi oceniać logi tekstowe oraz logi Windows Event ▪ Klasyfikuje wiadomości bazując	TAK	

	zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe.		
Cyberbezpieczeństwo			
1.	▪ System monitoruje urządzenia klasy UTM minimum w zakresie: – wykrywanie włamań i szybkość blokowania WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika – monitoruje stan synchronizacji klastra High-Availability. Status „zsynchronizowany" jest uważany za OK, a status „niezsynchronizowany" CRIT. – monitoruje ogólny stan alarmów czujników urządzenia Firewall. Status kontroli jest OK, jeśli wszystkie czujniki mają status alarmu „fałsz" (0) i CRIT, jeśli co najmniej jeden czujnik ma stan alarmu „prawda" (1). – monitoruje aktualną liczbę sesji na urządzeniu – monitoruje liczbę dostępnych tuneli IPSec VPN – monitoruje wykrywanie wirusów i szybkość blokowania systemów FortiGate AntiVirus. Przechodzi WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika. – monitoruje poziom wykorzystania procesora – Górne domyślne poziomy to 80,0, 90,0 procent. Poziomy są konfigurowalne. ▪ System ma możliwość odbierania i prezentacji danych z UTM z wykorzystaniem kolektora logów syslog ▪ System ma możliwość odbierania danych z systemu EDR z wykorzystaniem kolektora logów syslog.	TAK	
SOC i NOC			
1.	▪ Operacyjne Centrum Bezpieczeństwa; centrum kompetencyjne, które zajmować się będzie monitorowaniem infrastruktury teleinformatycznej, analizą zdarzeń, detekcją zagrożeń bezpieczeństwa i reagowaniem na wykryte incydenty naruszające bezpieczeństwo teleinformatyczne chronionych organizacji za pomocą analizy zbieranych logów z urządzeń, systemów IT oraz aplikacji, korelacją zdarzeń i detekcją zagrożeń oraz odpowiednią reakcję na pojawiające się incydenty ▪ W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie monitorowania zgodnie z opisanymi poniżej wymaganiami.	TAK	

	– Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa oraz ciągłości pracy infrastruktury w trybie 24 / 7 / 365, zgodnie z określonymi warunkami SLA. – Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji. – Analizę i eliminację najprostszych znanych zdarzeń określonych w ramach Scenariusza – Reakcji. – Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji. ▪ W ramach usługi Wykonawca monitoruje krytyczne elementy infrastruktury IT: – Serwery do 10 sztuk – Macierze do 4 sztuk, – Przełączniki SAN 2 sztuk – Przełączniki LAN 13 sztuk – Serwer Backupu 1 sztuk – Bibliotekę taśmowa LTO 1 sztuk – Macierz NAS 1 sztuk – UPS 12 sztuk – Serwerów aplikacji: – serwer AD 2 Sztuk ▪ W ramach usługi wykonawca monitoruje krytyczne elementy systemu HIS: – Monitorowanie komunikacji z platformą P1 w pełnym zakresie wymiany danych – Monitorowanie systemu HIS w zakresie wystawianych dokumentów EDM – Monitorowanie systemu HIS w zakresie pobieranej przez podmioty zewnętrzne z repozytorium dokumentacji EDM – Monitorowanie systemu His w ramach raportowania zdarzeń medycznych – Monitorowanie komunikacji modułu HL7 z poszczególnymi podsystemami zewnętrznymi i z ich rozgraniczeniem – Monitorowanie komunikacji EWUŚ – Monitorowanie KOWAL – Monitorowanie komunikacji AP-KOLCE – Monitorowanie RZM – Monitorowanie bazy danych systemu HIS – Monitorowanie środowiska Tomkat		

2. System EDR – do 200 stanowisk			
Lp.	**Wymagane minimalne parametry techniczne**	**Wymóg do spełnienia (warunek graniczny)**	**OFEROWANE PARAMETRY TECHNICZNE - podaje Wykonawca** **Wymogi dotyczące opisu oferowanych parametrów:** TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez

			wykonawcę NIE – wykonawca nie spełnia konkretnego parametru
Ochrona stacji roboczych - Windows			
1.	▪ Rozwiązanie musi wspierać systemy operacyjne Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11. ▪ Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows. ▪ Rozwiązanie musi wspierać architekturę ARM64. ▪ Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. ▪ Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. ▪ Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim. ▪ Skuteczność rozwiązania potwierdzona nagrodami VB100 i AV-comparatives.	TAK	
Ochrona antywirusowa i antyspyware			
1.	▪ Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. ▪ Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. ▪ Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami. ▪ Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje. ▪ Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. ▪ Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu. ▪ Rozwiązanie musi posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania. ▪ Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).	TAK	

	▪ Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. ▪ Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. ▪ Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych. ▪ Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. ▪ Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. ▪ Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku. ▪ Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. ▪ Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. ▪ Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera. ▪ W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. ▪ Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. ▪ Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. ▪ Rozwiązanie musi posiadać wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. ▪ Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. ▪ Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). ▪ Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. ▪ Rozwiązanie musi posiadać możliwość		

	opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. ▪ Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie. ▪ Rozwiązanie musi posiadać możliwość blokowania możliwości przeglądania wybranych stron internetowych. Rozwiązanie musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL. ▪ Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora. ▪ Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. ▪ Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. ▪ Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe. ▪ Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta. ▪ Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego. ▪ Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. ▪ Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym. ▪ Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. ▪ W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne. ▪ Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. ▪ Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń		

	do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie. ▪ Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika. ▪ Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. ▪ Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. ▪ Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. ▪ Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło. ▪ Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo. ▪ Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji. ▪ Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. ▪ Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń. ▪ System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. ▪ System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. ▪ Rozwiązanie musi posiadać umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. ▪ Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać		

	użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia. ▪ Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. ▪ Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia. ▪ Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. ▪ W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. ▪ Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika. ▪ Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS). ▪ Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. ▪ Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. ▪ Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. ▪ Rozwiązanie musi posiadać zaawansowany skaner pamięci. ▪ Rozwiązanie musi być wyposażone w		

	mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych. ▪ Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. ▪ Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. ▪ Rozwiązanie musi posiadać posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie. ▪ Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. ▪ Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera. ▪ Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji. ▪ Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. ▪ Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. ▪ Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). ▪ Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). ▪ Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym. ▪ W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania. ▪ Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym. ▪ Rozwiązanie musi być wyposażone w		

	dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń. ▪ Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji. ▪ Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline. ▪ Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie. ▪ W trakcie instalacji rozwiązanie ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM. ▪ W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji. ▪ Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej. ▪ Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia. ▪ Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny. ▪ Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. ▪ Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki. ▪ Rozwiązanie musi posiadać możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych. ▪ Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji. ▪ Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie. ▪ Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. ▪ Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.		

	▪ Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup. ▪ Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny. ▪ Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść". ▪ Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. ▪ Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. ▪ Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. ▪ Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. ▪ Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet. ▪ Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB. ▪ Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. ▪ Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.		
Ochrona przed spamem			
1.	▪ Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. ▪ Rozwiązanie musi umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. ▪ Rozwiązanie musi umożliwiać automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. ▪ Rozwiązanie musi posiadać możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego. ▪ Rozwiązanie musi posiadać możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego. ▪ Rozwiązanie musi posiadać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam. ▪ Rozwiązanie musi możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam. ▪ Rozwiązanie musi domyślnie współpracować z folderem „Wiadomości-śmieci", dostępnym	TAK	

	w programie Microsoft Outlook. ▪ Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana" ▪ Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana". ▪ Rozwiązanie musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.		
Zapora osobista (personal firewall)			
1.	▪ Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: – tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, – tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, – tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, – tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. ▪ Rozwiązanie musi oceniać reguły zapory systemu Windows. ▪ Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych. ▪ Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie. ▪ Rozwiązanie musi posiadać możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego. ▪ Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj. ▪ Rozwiązanie musi posiadać możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji. ▪ Rozwiązanie musi posiadać możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet. ▪ Rozwiązanie musi wykrywać modyfikację w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu. ▪ Rozwiązanie musi posiadać możliwość tworzenia profili pracy zapory osobistej w	TAK	

	zależności od wykrytej sieci. ▪ Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci. ▪ Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. ▪ Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie. ▪ Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6. ▪ Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci. ▪ Rozwiązanie musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów: – z aplikacją lokalną, którą administrator wskazuje z listy, – z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.		
Kontrola dostępu do stron internetowych			
1.	▪ Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. ▪ Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory. ▪ Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. ▪ Podstawowe kategorie, w jakie rozwiązanie musi być wyposażone to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. ▪ Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych. ▪ Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być	TAK	

	automatycznie aktualizowana przez producenta. ▪ Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych. ▪ Rozwiązanie musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj. ▪ Rozwiązanie musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.		
Bezpieczna przeglądarka			
1.	▪ Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. ▪ Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. ▪ Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki. ▪ Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę. ▪ Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki. ▪ Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.	TAK	
Ochrona serwera Windows			
1.	▪ Rozwiązanie musi posiadać wsparcie dla systemów Microsoft Windows Server 2008 R2 i nowszych. ▪ Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. ▪ Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. ▪ Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. ▪ Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami. ▪ Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje. ▪ Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. ▪ Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu. ▪ Rozwiązanie musi posiadać możliwość	TAK	

	utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). ▪ Rozwiązanie musi posiadać opcję skanowania „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. ▪ Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu. ▪ Rozwiązanie ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. ▪ Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych. ▪ Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. ▪ Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. ▪ Rozwiązanie musi wspierać mechanizm klastrowania. ▪ Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS). ▪ Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: – tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, – tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, – tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, – tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, – tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. ▪ Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. ▪ Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.		

	▪ Rozwiązanie musi posiadać zaawansowany skaner pamięci. ▪ Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych. ▪ Rozwiązanie musi oferować możliwość skanowania dysków sieciowych typu NAS. ▪ Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze. ▪ Rozwiązanie musi umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. ▪ Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. ▪ Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. ▪ Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia. ▪ Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. ▪ Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. ▪ W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. ▪ Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. ▪ Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. ▪ Dodanie automatycznych wyłączeń nie wymaga restartu serwera. ▪ Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. ▪ Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. ▪ Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po		

	instalacji. ▪ Rozwiązanie ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). ▪ Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. ▪ Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. ▪ Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie. ▪ Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. ▪ Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. ▪ Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. ▪ W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail. ▪ Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. ▪ Rozwiązanie musi posiadać możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło. ▪ Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo. ▪ Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji. ▪ Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje		

	▪ krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. ▪ Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń. ▪ System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. ▪ System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. ▪ Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. ▪ Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. ▪ Rozwiązanie musi oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. ▪ Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. ▪ Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera. ▪ Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji. ▪ Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. ▪ Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. ▪ Rozwiązanie musi być wyposażone w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). ▪ Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). ▪ Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. ▪ Rozwiązanie musi posiadać możliwość		

	wykluczania ze skanowania procesów. ▪ Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania. ▪ Rozwiązanie musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”. ▪ Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. ▪ Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia. ▪ Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. ▪ Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. ▪ Rozwiązanie musi posiadać ochronę przed przyłączeniem komputera do sieci botnet. ▪ Rozwiązanie musi mieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. ▪ Rozwiązanie musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów. ▪ Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. ▪ Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. ▪ Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. ▪ Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.		
Administracja zdalna			
1.	▪ Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019 oraz systemach Linux. ▪ Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD. ▪ Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego	TAK	

	serwera bazy danych MS SQL i MySQL. ▪ Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik. ▪ Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych. ▪ Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta. ▪ Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. ▪ Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy. ▪ Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6. ▪ Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs. ▪ Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji. ▪ Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. ▪ Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym. ▪ Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. ▪ Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. ▪ Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. ▪ Serwer administracyjny musi posiadać wsparcie dla „VDI" oraz „Golden Master Image". ▪ Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów. ▪ Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy. ▪ Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. ▪ Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. ▪ Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS. ▪ Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP. ▪ Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń		

	takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11. ▪ Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap. ▪ Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych. ▪ Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów. ▪ Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. ▪ Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi. ▪ Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android. ▪ Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS. ▪ Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci. ▪ Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. ▪ Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające. ▪ Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania. ▪ Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. ▪ Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać		

	określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny. ▪ W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play. ▪ Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. ▪ Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS. ▪ Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego. ▪ Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi. ▪ Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. ▪ Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. ▪ Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. ▪ Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej. ▪ Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany. ▪ Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej. ▪ Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji. ▪ Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z		

	użyciem parametrów instalacyjnych. ▪ Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. ▪ Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej. ▪ Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. ▪ Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. ▪ Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. ▪ Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania. ▪ Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. ▪ Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta. ▪ Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej. ▪ Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji. ▪ Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce. ▪ Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta. ▪ Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów. ▪ Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie. ▪ Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy. ▪ Serwer administracyjny musi posiadać		

	możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania. ▪ Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów. ▪ Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny. ▪ Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może ▪ zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF lub CSV. ▪ Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. ▪ Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów. ▪ Powiadomienia mailowe mają być wysyłane w formacie HTML. ▪ Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń. ▪ Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog. ▪ Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu. ▪ Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji. ▪ Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami. ▪ Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych. ▪ W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu. ▪ Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela. ▪ Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan. ▪ Serwer musi umożliwić podział uprawnień		

	administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami. ▪ Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli. ▪ W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych. ▪ Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta. ▪ Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli. ▪ Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania. ▪ Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie. ▪ Konsola administracyjna musi umożliwiać personalizację interfejsu webowego. ▪ Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych. ▪ 9Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault). ▪ Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk. ▪ Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal). ▪ Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.		
Sandbox w chmurze			
1.	▪ Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. ▪ Rozwiązanie musi wykorzystywać do działania chmurę producenta. ▪ Rozwiązanie musi posiadać możliwość	TAK	

	określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. ▪ Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. ▪ Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. ▪ Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. ▪ Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. ▪ Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. ▪ Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. ▪ Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. ▪ Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. ▪ Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: – Czysty, – Podejrzany, – Bardzo podejrzany, – Szkodliwy. ▪ W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. ▪ 1W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.		
Endpoint Detection and Response			
	Serwer ▪ Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych. ▪ Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. ▪ System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta. ▪ Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.		

	▪ Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych. ▪ Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. ▪ Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. ▪ Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. ▪ Wykluczenia muszą dotyczyć procesu lub procesu „rodzica". ▪ Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. ▪ Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. ▪ Serwer musi posiadać ponad 800 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. ▪ Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne. ▪ Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. ▪ Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali. ▪ Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. ▪ Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. ▪ Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. ▪ W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. ▪ W ramach przeglądania wykonanego skryptu		

	lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. ▪ Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy. ▪ Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich. ▪ Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal). ▪ Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. ▪ Konsola administracyjna musi mieć możliwość tagowania obiektów. ▪ Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli. ▪ Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci. ▪ Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell. ▪ Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł. **Agent** ▪ Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10 oraz Windows Server 2008/2012/2016/2019. ▪ Pełne wsparcie dla systemów macOS 10.12 i nowszych. ▪ Wsparcie dla 32 i 64-bitowej wersji systemu Windows. ▪ Agent musi współpracować z produktem antywirusowym tego samego producenta. ▪ Agent nie może działać bez produktu antywirusowego tego samego producenta. ▪ W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonanej przez		

	agenta. ▪ Połączenie agenta do serwera zarządzającego musi być szyfrowane. ▪ Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane.		

3. Skan podatnośći			
Lp.	**Wymagane minimalne parametry techniczne**	**Wymóg do spełnienia (warunek graniczny)**	**OFEROWANE PARAMETRY TECHNICZNE - podaje Wykonawca** **Wymogi dotyczące opisu oferowanych parametrów:** TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę NIE – wykonawca nie spełnia konkretnego parametru
1.	▪ Wykonanie skanów otwartych portów w całej adresacji publicznej audytowanego podmiotu. ▪ Wykorzystanie dedykowanego oprogramowania do wykrywania podatności zasilonego ▪ najnowszą bazą znanych podatności. ▪ Wykonanie skanów nieuwierzytelnionych. ▪ Wykonanie raportu końcowego. **Planowanie (faza I)** ▪ Rekonesans, kolekcja danych i pozyskiwanie informacji, mapowanie **Testy stabilności i dostępności infrastruktury sieciowej na styku z Internetem (faza II)** ▪ Skan całej puli adresacji publicznej jednostki audytowanej ▪ Testy ekspozycji systemów na styku z Internetem ▪ Opcjonalne testy destabilizujące infrastrukturę sieciową typu Denial of Service ▪ W sytuacji wykrycia mniejszej bądź większej liczby systemów niż w przyjętych w punkcie ▪ „założenia skali i architektury przyjęte w wycenie”, nastąpi spotkanie między ▪ zamawiającym, a wykonawcą, które będzie miało na celu doprecyzowanie danych lub ▪ przekazanie dodatkowych informacji wykonawcy **Raportowanie (faza III)** ▪ Zebranie wyników testów bezpieczeństwa ▪ Analiza wyników audytu ▪ Opisanie podatności wraz z kategoryzacją CVE i CVSS	TAK	

	▪ Opisanie rekomendacji ▪ Przekazanie raportu ▪ Zawartość raportu: ▪ Executive Summary – główne konkluzje ▪ Główne rekomendacje ▪ Przedmiot testów ▪ Risk Rating ▪ Metodologia i kryteria testowania ▪ Wykorzystane narzędzia w trakcie prowadzenia skanów ▪ Wykaz zidentyfikowanych podatności wraz z odpowiadającym im kodem CVE ▪ (Common Vulnerability Enumaration) oraz odnośnikiem do opisu luki. ▪ Podatności będą pogrupowane według ryzyka, zgodnie ze standardem CVSS ▪ (Common Vulnerability Scoring System). ▪ Rekomendacje związane z możliwym usunięciem wykrytych podatności		
Istotne założenia			
1.	▪ Typ prowadzonego audytu: Black Box / Grey Box ▪ W momencie konieczności przeprowadzenia skanu uwierzytelnionego wykonawca ma prawo uzyskać od jednostki audytowanej poświadczenia dla danego systemu. Będzie to warunkiem prowadzenia skanu uwierzytelniającego. Brak przekazania poświadczeń uwierzytelniających nie będzie podstawą do wstrzymania audytu. ▪ W ramach testów nie jest przewidziana próba przełamania zabezpieczeń fizycznych lub sprawdzenia reakcji służb bezpieczeństwa zamawiającego na nieautoryzowany dostęp ▪ Zespół testerów dołoży wszelkich starań w trakcie pozyskiwania informacji i testowania w celu zminimalizowania ingerencji w sieć produkcyjną. Jednak działania testerów mogą być obarczone pewnym prawdopodobieństwem destabilizacji niektórych usług, o czym wykonawca powiadomi zamawiającego przed wykonaniem danego testu. ▪ Działania audytowe mogą być prowadzone o dowolnej porze dnia i nocy. ▪ Przed rozpoczęciem prac audytowych niezbędne będzie wypełnienie stosownej deklaracji osób decyzyjnych zamawiającego oraz jednostki audytowanej świadczącej o zgodzie na działania i wiedzy nt. potencjalnych skutków działań testerów. ▪ Testowanie odbędzie się zdalnie z biura oraz centrum przetwarzania danych wykonawcy ▪ Audyt danej jednostki zostaje zakończony w momencie przekazania raportu zamawiającemu jako zaszyfrowany załącznik w wiadomości Email ▪ Tester użyje komputera niepowiązanego z podmiotem audytowanym przy próbach dostępu do zasobów	TAK	

4. Serwer bazodanowy			
Lp.	**Wymagane minimalne parametry techniczne**	**Wymóg do spełnienia (warunek graniczny)**	**OFEROWANE PARAMETRY TECHNICZNE - podaje Wykonawca** **Wymogi dotyczące opisu oferowanych parametrów:** TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę NIE – wykonawca nie spełnia konkretnego parametru
1.	obudowa do montażu w szafie typu rack	TAK	
2.	zasilanie redundantne, przynajmniej 2 zasilacze typu HotPlug	TAK	
3.	płyta główna z możliwością zainstalowania minimum dwóch procesorów	TAK	
4.	zegar procesora minimum 2,6 GHz	TAK	
5.	zainstalowany 1 procesor minimum ośmiordzeniowy klasy x86 dedykowane do pracy w serwerach, zaprojektowane do pracy w układach wieloprocesorowych	TAK	
6.	pamięć minimum 128GB ECC DIMM, rozszerzalna, z zabezpieczeniem typu: ECC	TAK	
7.	dyski minimum 2x 960 GB SSD skonfigurowane w RAID1 , 6x8TB 7.2K	TAK	
8.	sieć minimum 2x16Gb FC, 2x10Gb SFP+ SR	TAK	
9.	z przodu obudowy: 1x USB 3.0, 1x USB 2.0	TAK	
10.	z tyłu obudowy: 2x USB 3.0, , 1x DB-15	TAK	
11.	Zarządzanie: – Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania – Monitoring statusu i zdrowia systemu – Logowanie zdarzeń – Umożliwiający Update systemowego firmware – Umożliwiający zdalną konfigurację serwera – Monitoring i możliwość ograniczenia poboru prądu – Zdalne włączanie/wyłączanie/restart – Przekierowanie konsoli szeregowej przez IPMI – Zrzut ekranu w momencie zawieszenia system – Możliwość przejęcia zdalnego ekranu 1920x1200, 60 Hz,16 bpp – Zdalny dostęp do serwera – Możliwość zdalnej instalacji systemu operacyjnego – Alerty Syslog		

	– Przekierowanie konsoli szeregowej przez SSH – Wyświetlanie danych aktualnych I historycznych dla użycia energii I temperatury serwera – Możliwość mapowania obrazów ISO z lokalnego dysku operatora – Możliwość mapowania obrazów ISO przez HTTPS – Możliwość jednoczesnej pracy użytkowników przez wirtualną konsolę – Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3		
12.	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID	TAK	
13.	gwarancja: min. 36 m-cy , 3YNBD, producenta	TAK	

5. Biblioteka taśmowa

Lp.	**Wymagane minimalne parametry techniczne**	**Wymóg do spełnienia (warunek graniczny)**	**OFEROWANE PARAMETRY TECHNICZNE - podaje Wykonawca** **Wymogi dotyczące opisu oferowanych parametrów:** TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę NIE – wykonawca nie spełnia konkretnego parametru
Wymagania techniczne			
1.	Obudowa przystosowana do montażu w standardowej szafie rack 19''. Maksymalna wysokość oferowanego rozwiązania - 3U.		
2.	Biblioteka taśmowa musi być wyposażona w min. 1 napęd taśmowy LTO8 z interfejsem FC min. 8 Gbit/s.		
3.	Biblioteka taśmowa musi mieć możliwość rozbudowy do min. 8 napędów taśmowych.		
4.	Biblioteka musi być wyposażona w nie mniej niż 20 slotów na taśmy i posiadać możliwość rozbudowy do co najmniej 100 slotów na taśmy.		
5.	Biblioteka musi być wyposażona w przynajmniej 3 sloty wejścia/wyjścia, umożliwiający wymianę taśm bez konieczności wyłączania urządzenia.		
6.	Biblioteka musi być wyposażona w czytnik kodów kreskowych.		
7.	Biblioteka musi być wyposażona w komplet magazynków na taśmy, tak by możliwa była pełna obsada biblioteki taśmami LTO.		
8.	Możliwość zdalnego zarządzania biblioteką poprzez interfejs WWW.		

9.	Możliwość monitorowania stanu biblioteki i napędów.		
10.	Biblioteka musi posiadać panel sterowania oraz wyświetlacz informujący o błędach urządzenia, aktywności napędów.		
Wymagania dodatkowe			
11.	Do biblioteki należy dostarczyć: - niezbędne kable zasilające, - taśmę LTO 8 – 10 szt. - taśmę czyszczącą – 1 szt. - przewód światłowodowy – 1 szt.		
12.	Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu.		
13.	Wszystkie oferowane urządzenia muszą być fabrycznie nowe.		
14.	Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.		
15.	Urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.		
16.	Oferowane produkty (urządzenia, sprzęty) w przedmiotowym postępowaniu o udzielenie zamówienia publicznego muszą spełniać wymagania norm CE, tj. muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE.		
17.	Urządzanie musi być objęta 36 miesięczną gwarancją		
18.	Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia przez cały okres obowiązywania gwarancji.		

6. System Backupowy			
Lp.	**Wymagane minimalne parametry techniczne**	**Wymóg do spełnienia (warunek graniczny)**	**OFEROWANE PARAMETRY TECHNICZNE - podaje Wykonawca** **Wymogi dotyczące opisu oferowanych parametrów:** TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę NIE – wykonawca nie spełnia konkretnego parametru
1. MECHANIZMY ZABEZPIECZANIA DANYCH			
Ogólne			

1.	Rozwiązanie musi mieć możliwość konfigurowania liczby równoległych wątków wykonujących zadania tworzenia kopii zapasowej i odtwarzania		
2.	Rozwiązanie musi umożliwiać bezagentowe (bez konieczności instalowania agenta w zabezpieczanym systemie operacyjnym) zabezpieczenie środowisk wirtualnych, kontenerowych , aplikacji, lub instancji pamięci masowej (wolumenu lub systemu plików)		
3.	Mechanizm tworzenia oraz odtwarzania maszyn wirtualnych musi być spójny dla wszystkich wymienionych platform wirtualizacyjnych pod kątem konfiguracji.		
4.	Architektura rozwiązania powinna umożliwiać skalowanie horyzontalne (ang. scale-out) komponentów realizujących proces kopii zapasowej (ang. data-mover)		
5.	System powinien przechowywać wszystkie metadane kopii zapasowych w relacyjnej bazie danych		
6.	System powinien umożliwiać konfigurację w klastrze active-passive (komponent zarządzający rozwiązaniem)		
7.	System powinien umożliwiać pracę w trybie autonomicznym (bez konieczności instalowania innych systemów backupów)		
8.	Rozwiązanie musi umożliwić zarówno ręczne odtworzenie pojedynczej maszyny wirtualnej jak I zaplanowanie masowego odtworzenia wielu maszyn wirtualnych do wskazanego z góry środowiska (na żądanie oraz cyklicznie z opcją nadpisania istniejących maszyn wirtualnych)		
9.	Rozwiązanie powinno umożliwiać automatyczne wysyłanie raportów do centralnej bazy producenta (opcjonalnie z zawartością logów) w celu usprawnienia diagnostyki i świadczenia wsparcia przez producenta		
Vmware vSphere/ESXi			
10.	Obsługa Vmware vSphere/ESXi od wersji 6 korzystając z „VMware vSphere Storage API”.		
11.	Wykonywanie kopii zapasowych w oparciu o technologie NBD & HotAdd.		
12.	Wykonywanie przyrostowych kopii zapasowych z wykorzystaniem mechanizmu CBT.		
13.	Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji		
14.	Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej		
15.	Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI.		
16.	Możliwość pominięcia wybranych dysków		

	maszyny wirtualnej z kopii zapasowej		
17.	Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki)		
18.	Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o przypisane w środowisku tagi.		
19.	Możliwość automatycznego wykonania polecenia na maszynie wirtualnej (której kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej.		
20.	Możliwość wykonywania cyklicznie migawek maszyny wirtualnej bez eksportu danych i ich automatyczna rotacja (usuwanie najstarszych – polityka powinna umożliwiać wskazanie liczby migawek i okres przez jaki powinny być przetrzymywane)		
21.	Możliwość użycia migawek spójnych na poziomie aplikacji (ang. quiesced snapshot) przy wykonywaniu kopii zapasowej		
22.	Możliwość automatycznego uruchomienia maszyny wirtualnej po zakończonym procesie odtwarzania.		
Oracle VM			
23.	Obsługa Oracle VM od wersji 3.4 wzwyż.		
24.	Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji		
25.	Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej		
26.	Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI.		
27.	Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej		
28.	Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki)		
29.	Możliwość tworzenia pełnych kopii zapasowych maszyn wirtualnych w oparciu o migawki (ang. snapshot)		
AWS EC2			
30.	Wsparcie dla AWS EC2		
31.	Możliwość odtworzenia całej maszyny wirtualnej		

	na środowisko wirtualizacji		
32.	Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej		
33.	Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI.		
34.	Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej		
35.	Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki)		
36.	Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o przypisane w środowisku tagi.		
37.	Możliwość tworzenia pełnych kopii zapasowych maszyn wirtualnych w oparciu o migawki (ang. snapshot)		
38.	Możliwość automatycznego wykonania polecenia na maszynie wirtualnej (której kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej.		
39.	Możliwość wykonania migawki (snapshot).		
40.	Możliwość automatycznego uruchomienia maszyny wirtualnej po zakończonym procesie odtwarzania.		
Aplikacje			
41.	Rozwiązanie musi umożliwiać wykonanie kopii zapasowej przy użyciu natywnych poleceń zabezpieczanej aplikacji (wykonujących np. spójną kopię zapasową bazy danych) na zdalnych maszynach oraz poprzez opracowane dedykowane skrypty administracyjne bez konieczności wykonania obrazu całej maszyny wirtualnej lub instancji pamięci masowej (wolumenu lub systemu plików)		
42.	Rozwiązanie musi umożliwiać zdefiniowanie w jaki sposób kopia zapasowa będzie wykonana (jakie polecenie, jakie parametry, gdzie znajdują się pliki do zabezpieczenia) a następnie umożliwiać wielokrotne przypisanie takiej konfiguracji do wielu instancji aplikacji z różnymi wartościami parametrów, tak aby nie było konieczności wielokrotnego podawania argumentów polecenia dla każdej z aplikacji z osobna		
43.	Rozwiązanie musi umożliwiać wykonywanie skryptów i poleceń zarówno poprzez SSH (zdalnie) jak i z maszyny na której jest zainstalowane rozwiązanie producenta (tak, żeby nie było konieczności uruchamiania usług		

	zdalnych takich jak SSH w celu wykonania kopii zapasowej)		
44.	Rozwiązanie powinno umożliwiać wkopiowanie danych backupu do innego systemu z użyciem SSH – np. transfer danych kopii zapasowej z aplikacji produkcyjnej na środowisko aplikacji testowej		
File System			
45.	Możliwość wykonywania kopii zapasowych filesystemu podłączonego do noda vProtect (katalogi, pliki zwykłe, dowiązania symboliczne)		
46.	Możliwość wykonania kopii zapasowej pełnej.		
47.	Możliwość wykonania kopii zapasowej przyrostowej.		
48.	Możliwość odtworzenia pojedynczego pliku.		
49.	Możliwość podłączenia zasobu po interfejsie ISCSI, jako dysk z filesystemem XFS.		
Nutanix Files (AFS)			
50.	Możliwość wykonywania kopii zapasowych Nutanix Files (AFS), zasobów NFS/SMB, z wykorzystaniem funkcjonalności CFT.		
51.	Możliwość wykonania kopii zapasowej pełnej.		
52.	Możliwość wykonania kopii zapasowej przyrostowej.		
53.	Możliwość odtworzenia pojedynczego pliku.		
54.	Możliwość podłączenia zasobu po interfejsie ISCSI, jako dysk z filesystemem XFS.		
Ceph RBD			
55.	Możliwość wykonania kopii zapasowych wolumenów Ceph RBD.		
56.	Możliwość wykonania kopii zapasowej pełnej.		
57.	Możliwość wykonania kopii zapasowej przyrostowej.		
58.	Możliwość odtworzenia pojedynczego pliku.		
59.	Możliwość podłączenia zasobu po interfejsie ISCSI		
60.	Możliwość wykonywania cyklicznie migawek wolumenu bez eksportu danych i ich automatyczna rotacja (usuwanie najstarszych – polityka powinna umożliwiać wskazanie liczby migawek i okres przez jaki powinny być przetrzymywane)		
61.	Możliwość automatycznego wykonania polecenia bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej.		

62.	Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa wolumenów RBD (np. wolumeny RBD o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki)		
7. SKŁADOWANIE DANYCH KOPII ZAPASOWYCH			
Ogólne			
1.	Rozwiązanie musi umożliwiać wykonanie polecenia/skryptu administracyjnego przed i po dostępie do pamięci masowej – np. w celu wywołania mechanizmów replikacji danych lub wysyłania powiadomień		
2.	Rozwiązanie musi umożliwiać synchronizację obecności kopii zapasowej w danej lokalizacji składowania z wewnętrzna bazą danych, np. gdyby ręcznie kopie zostały usunięte, nie powinny widnieć w interfejsie użytkownika; analogicznie gdyby ponownie były dostępne, np. po tymczasowej awarii systemu plików, powinny ponownie zostać zaznaczone jako dostępne		
System plików			
3.	Rozwiązanie musi umożliwiać składowanie kopii zapasowej na lokalnych lub zdalnych zasobach dyskowych podmontowanych do rozwiązania jako systemy plików		
4.	Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii)		
5.	Rozwiązanie musi oferować deduplikację danych		
6.	Rozwiązanie musi oferować szyfrowanie danych kluczem generowanym przez rozwiązanie		
7.	Rozwiązanie powinno umożliwiać wykorzystanie mechanizmu ochrony nadpisania zabezpieczonych kopii zapasowych (ang. retention lock), gdy używany jest Dell-EMC PowerProtect (DataDomain)		
System plików (syntetyczny)			
8.	Rozwiązanie musi umożliwiać składowanie kopii zapasowej na lokalnych lub zdalnych zasobach dyskowych podmontowanych do rozwiązania jako systemy plików		
9.	Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii)		
10.	Rozwiązanie musi umożliwiać składować dane w postaci syntetycznej bez konieczności scalania przyrostowych kopii zapasowych w trakcie odtwarzania		

IBM Spectrum Protect			
11.	Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie IBM Spectrum Protect od wersji 7		
12.	Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii)		
13.	Rozwiązanie musi oferować deduplikację danych po stronie zarówno rozwiązania jak i serwera IBM Spectrum Protect		
Dell EMC Avamar			
14.	Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie Dell EMC Avamar od wersji 7.5		
15.	Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii)		
16.	Integracja powinna używać narzędzi administracyjnych dostarczanych przez Dell EMC		
Dell EMC NetWorker			
17.	Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie Dell EMC NetWorker od wersji 9		
18.	Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii)		
19.	Integracja powinna używać narzędzi administracyjnych dostarczanych przez Dell EMC		
Veritas NetBackup			
20.	Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie Versitas NetBackup od wersji 7.6		
21.	Rozwiązanie musi oferować deduplikację danych po stronie serwera Veritas NetBackup		
Amazon S3 **Scality S3** **IBM Cloud Object Storage** **Alibaba Cloud OSS** **Claudian S3**			
22nd	Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie pamięci masowej oferowanej z użyciem interfejsu obiektowego S3		
23.	Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii)		

24.	Rozwiązanie musi umożliwiać przenoszenie starszych kopii zapasowych z Amazon S3 do Amazon Glacier w celu redukcji kosztów przechowywania danych		
25.	Rozwiązanie musi oferować szyfrowanie danych kluczem generowanym przez rozwiązanie		
26.	Rozwiązanie musi umożliwiać wsparcie dla systemów które wspierają wersjonowanie oraz takich, które nie posiadają takiej możliwości		
Microsoft Azure Blob			
27.	Rozwiązanie musi umożliwiać składowanie kopii zapasowej w chmurze pamięci masowej Microsoft Azure Blob		
28.	Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii)		
29.	Rozwiązanie musi oferować szyfrowanie danych kluczem generowanym przez rozwiązanie		
Google Cloud Storage			
30.	Rozwiązanie musi umożliwiać składowanie kopii zapasowej w chmurze pamięci masowej Google Cloud Storage		
31.	Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii)		
32.	Rozwiązanie musi oferować szyfrowanie danych kluczem generowanym przez rozwiązanie		
OpenStack Swift			
33.	Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie pamięci masowej oferowanej z użyciem interfejsu obiektowego Swift w wersji 3		
34.	Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii)		
35.	Rozwiązanie musi oferować kompresję danych przed składowaniem ich w Swift		
Biblioteki Taśmowe			
36.	Obsługa bibliotek taśmowych fc/sas , mozliwość ustawienia retencji , oraz zapisu jednoprzebiegowego – kopia wykonywana raz zapisywana najpierw na dysk I potem na taśmę (disk 2 disk 2 tape)		
3. INTERFEJS ADMINISTRACYJNY I API			
Ogólne			

1.	Rozwiązanie musi oferować możliwość dostęp administracyjny za pośrednictwem interfejsu web'owego (przeglądarka internetowa), tekstowego (CLI) oraz API		
2.	Interfejsy powinny umożliwiać administratorom logowanie z użyciem poświadczeń Active Directory lub LDAP		
3.	System powinien umożliwiać nadawanie uprawnień i dostępów administratorom do na podstawie definiowalnych ról (ang. RBAC) na poziomie globalnym systemu (sekcji interfejsu użytkownika) oraz do poszczególnych instancji środowisk wirtualnych, aplikacji i instancji pamięci masowych (wolumenów lub systemów plików)		
Interfejs webowy			
4.	Interfejs musi umożliwiać wyświetlenie podstawowych statystyk, czy dane środowisko wirtualne lub aplikacja jest zabezpieczona		
5.	Interfejs musi umożliwiać wyświetlenie statystyk prędkości wykonywania kopii (ilość danych w jednostce czasu) i czasu trwania, czy dane środowisko wirtualne lub aplikacja jest zabezpieczona z podziałem na fazy wykonywania zadań kopii zapasowych (eksport danych ze środowiska i zapis w miejscu składowania danych)		
6.	Interfejs musi umożliwiać konfigurację cyklicznie przesyłanych raportów ze statusem ostatnio wykonanych kopii zapasowych		
7.	Interfejs musi umożliwiać konfigurację cyklicznie przesyłanych raportów ze statusem kopii zapasowych, które nie powiodły się w ostatnim czasie – np. w ciągu ostatnich kilkunastu minut, niedostępności komponentu wykonującego kopie zapasowe (ang. data-mover)		
8.	Interfejs musi umożliwiać wyświetlenie statystyk takich jak rozmiar kopii zapasowej oraz czas potrzebny na wykonanie kopii zapasowej lub odtworzenia w perspektywie czasu, np. w celu analizy przyrostu rozmiarów backupu lub czasu jego wykonywania		
9.	Interfejs powinien umożliwiać raportowanie zajętość przestrzeni dyskowej w miejscach składowania danych z podziałem na środowiska wirtualne, polityki, maszyny wirtualne, instancje pamięci masowej		
10.	Interfejs musi umożliwiać centralne zarządzanie konfiguracją komponentów realizujących proces kopii zapasowej (ang. data-mover), danych dostępowych i metod wykonywania kopii zapasowych wirtualizatorów oraz konfiguracji miejsc składowania danych		

11.	Interfejs musi umożliwiać wykonanie na żądanie kopii zapasowej wskazanego środowiska, aplikacji lub instancji pamięci masowej (systemu plików lub wolumenu)		
12.	Interfejs musi umożliwiać wykonanie odtworzenia kopii zapasowej wskazanego środowiska lub instancji pamięci masowej (systemu plików lub wolumenu)		
13.	Interfejs musi umożliwiać wykonanie operacji montowania kopii zapasowej w celu dostępu do pojedynczych plików (jeśli wspierane dla danego wirtualizatora) – odtworzenie plików lub folderów musi również odbywać się za pośrednictwem interfejsu web'owego		
14.	Interfejs musi umożliwiać konfigurację cyklicznego wykonywania kopii zapasowej wskazanych środowisk wirtualnych, aplikacji, instancji pamięci masowej (systemu plików lub wolumenu), migawek środowisk wirtualnych oraz okresowego przywracania wskazanych maszyn wirtualnych		
15.	Harmonogramy cyklicznego wykonywania kopii zapasowych, migawek i przywracania środowisk wirtualnych powinny umożliwiać wskazywanie: godziny rozpoczęcia, dni tygodnia oraz ich kolejne wystąpienie w miesiącu (np. drugi wtorek miesiąca), miesiące		
16.	Harmonogramy cyklicznego wykonywania kopii zapasowych, migawek i przywracania środowisk wirtualnych powinny umożliwiać interwałowe wykonywania zadania - wskazywanie: godziny rozpoczęcia, i godziny zakończenia i odstępu		
17.	Interfejs musi umożliwiać monitorowanie na żywo postępu i ewentualne anulowanie zadań wykonywanych przez rozwiązanie		
18.	Interfejs musi umożliwiać szybkie wyszukiwanie elementów konfiguracji, środowisk wirtualnych, aplikacji i instancji pamięci masowej (systemu plików lub wolumenu)		
19.	Interfejs musi udostępniać kreatora konfiguracji podstawowych elementów rozwiązania takich jak dodanie środowiska wirtualnego, rozwiązań pamięci masowych, polityk i harmonogramów		
20.	Interfejs powinien umożliwiać wykonanie testu połączenia ze środowiskiem zabezpieczanym oraz miejsca składowania kopii zapasowych		
Interfejs tekstowy			
21.	Interfejs musi umożliwiać wyświetlenie podstawowych statystyk, czy dane środowisko wirtualne lub aplikacja jest zabezpieczona		
22.	Interfejs musi umożliwiać wykonanie na żądanie kopii zapasowej wskazanego środowiska, aplikacji, lub instancji pamięci masowej (systemu plików lub wolumenu)		
23.	Interfejs musi umożliwiać wykonanie na odtworzenia kopii zapasowej wskazanego		

	środowiska lub instancji pamięci masowej (systemu plików lub wolumenu)		
24.	Interfejs musi umożliwiać wykonanie operacji montowania kopii zapasowej w celu dostępu do pojedynczych plików (jeśli wspierane dla danego wirtualizatora) – odtworzenie plików lub folderów musi wówczas odbywać się bezpośrednio ze wskazanej ścieżki na systemie rozwiązania		
25.	Interfejs musi umożliwiać konfigurację cyklicznego wykonywania kopii zapasowej wskazanych środowisk wirtualnych lub aplikacji, migawek środowisk wirtualnych oraz okresowego przywracania wskazanych maszyn wirtualnych		
26.	Interfejs musi umożliwiać monitorowanie postępu i ewentualne anulowanie zadań wykonywanych przez rozwiązanie		
27.	Interfejs tekstowy musi być umożliwiać wykonywanie poleceń w trybie nie-interakcyjnym (z poziomu skryptu)		
Interfejs programistyczny (API)			
28.	Rozwiązanie musi umożliwiać pełną konfigurację, wykonywanie wszystkich operacji oraz odczyt wszystkich dostępnych statystyk z poziomu API		
29.	Rozwiązanie musi udostępniać wszystkie API z użyciem technologii REST i JSON		

Wymagania w zakresie instalacji i konfiguracji serwera, biblioteki i systemu backupowego

1. Montaż serwerów w posiadanej szafie rack 42U w pomieszczeniu udostępnionym przez Zamawiającego.
2. Podłączenie serwera i biblioteki do listw zasilających PDU.
3. Aktualizacja oprogramowania układowego wszystkich komponentów.
4. Podłączenie do sieci LAN (rekonfiguracja przełączników)
5. Konfiguracja RAID serwera.
6. Instalacja i konfiguracja systemu operacyjnego.
7. Konfiguracja systemu zdalnego zarządzania.
8. Instalacja , uruchomienie i konfiguracja systemu backupowego.
9. Opracowanie polityki backupu .
10. Wymagane jest wykonanie testowego backupu oraz odtworzenia z weryfikacją prawidłowości działania systemów odtworzonych .
11. Wykonawca po zainstalowaniu i skonfigurowaniu sprzętu i oprogramowania będzie miał obowiązek przeprowadzenia instruktażu dla administratorów Zamawiającego w zakresie konfiguracji i zarządzania dostarczonego sprzętu oraz oprogramowania.

8. System do zapisywania zdarzeń oraz raportowania			
Lp.	**Wymagane minimalne parametry techniczne**	**Wymóg do spełnienia (warunek graniczny)**	**OFEROWANE PARAMETRY TECHNICZNE - podaje Wykonawca** **Wymogi dotyczące opisu oferowanych parametrów:** TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę NIE – wykonawca nie spełnia konkretnego parametru

Interfejsy, Dysk, Zasilanie:			
1.	System musi dysponować co najmniej: • 2 portami Gigabit Ethernet RJ-45.		
2.	Rozwiązanie musi dysponować powierzchnią dyskową min. 4 TB		
3.	System musi być wyposażony w zasilanie AC		
Parametry wydajnościowe:			
4.	System musi być w stanie przyjmować minimum 25 GB logów na dzień		
5.	System musi być w stanie przeanalizować minimum 500 logów na sekundę.		
6.	Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 50 systemów.		
Logowanie:			
7	Podgląd logowanych zdarzeń w czasie rzeczywistym.		
8.	Możliwość przeglądania logów historycznych z funkcją filtrowania.		
9.	System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: a. Listę najczęściej wykrywanych ataków. b. Listę najbardziej aktywnych użytkowników. c. Listę najczęściej wykorzystywanych aplikacji. d. Listę najczęściej odwiedzanych stron www. e. Listę krajów , do których nawiązywane są połączenia. f. Listę najczęściej wykorzystywanych polityk Firewall. g. Informacje o realizowanych połączeniach IPSec.		
10.	Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.		

11.	Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.		
12.	System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.		
Raportowanie:			
13.	Generowanie raportów co najmniej w formatach: PDF, CSV.		
14.	Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.		
15.	Funkcję definiowania własnych raportów.		
16.	Możliwość spolszczenia raportów.		
17.	Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.		
Korelacja logów:			
18.	Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.		
19.	Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.		
20.	Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie VPN, utracone połączenie sieciowe.		
Zarządzanie:			
21.	System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która		

	komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.		
22.	System musi umożliwiać definiowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi..		
Serwisy i licencje:			
23.	1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.		

Aktualizacja procedur bezpieczeństwa

Opracowania/uaktualnienie wraz z przekazaniem praw autorskich dokumentacji systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070), rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), oraz ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655)

Szkolenia

Przeprowadzenie szkoleń (stacjonarnych lub online jeśli warunki epidemiologiczne nie pozwolą na szkolenia stacjonarne) w zakresie cyberbezpieczeństwa skierowanych do kadry zarządzającej świadczeniodawcą oraz osób zatrudnionych u świadczeniodawcy w zakresie podstawowej świadomości bezpieczeństwa IT (w 2 terminach), w tym:

a) ochrony przed zaawansowanymi atakami przez pocztę i WWW,

b) tworzenia i zarządzania polityką haseł i tożsamości,

c) zarządzania ryzykiem, dokumentacją i polityką bezpieczeństwa w jednostkach publicznych w świetle rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247),

d) wykonywania kopii zapasowych oraz tworzenia i utrzymania polityki ciągłości działania.