**GMINA WRONKI**

**Ul. Ratuszowa 5, 64-510Wronki
NIP 7631002006, REGON 570791460**

*pt. „e-usługi publicznej dla mieszkańców Gminy Wronki”*



Opis Przedmiotu Zamówienia (OPZ)

dot. zakupu sprzętu informatycznego i oprogramowania narzędziowego

Wronki, 26.06.2024 r.

WYKAZ

[1. Środki trwałe 2](#_Toc170282230)

[1.1 Sprzęt serwerowy wraz z oprogramowaniem i wdrożeniem – 1 szt. 2](#_Toc170282231)

[2. Wartości niematerialne i prawne 6](#_Toc170282232)

[2.1 Red Hat Enterprise Linux Server lub równoważny 6](#_Toc170282233)

[2.2 Windows Server 2022 Standard lub równoważny – 12 szt. (1 komplet) 7](#_Toc170282234)

[2.3 Windows Server 2022 External Connector lub równoważny – 1 szt. 8](#_Toc170282235)

[2.4 Certyfikaty serwerowe 9](#_Toc170282236)

[2.5 Oprogramowanie antywirusowe z wbudowanym systemem EDR – 1 szt. 10](#_Toc170282237)

[2.6 Oprogramowanie w zakresie cyberbezpieczeństwa 1- szt. 17](#_Toc170282238)

[3. Instalacja i konfiguracja urządzeń 20](#_Toc170282239)

# ŚRODKI TRWAŁE

## 1.1 Sprzęt serwerowy wraz z oprogramowaniem i wdrożeniem – 1 szt.

|  |  |
| --- | --- |
| Element konfiguracji | Wymagania minimalne |
| Obudowa | Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia).Serwer z zainstalowanym przednim panelem oraz zamkiem chroniącym przed nieuprawionym dostępem do dysków oraz czujnikiem otwarcia obudowy współpracującego z BIOS/UEFI.  |
| Procesor | Procesory ośmio-rdzeniowe, x86 - 64 bity, pracujące z częstotliwością bazową min. 2.8GHz i osiągające w testach SPECrate2017\_int\_base wynik nie gorszy niż 132 punkty, dla testu oferowanego modelu serwera z 2 procesorami. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.orgPłyta główna wspierająca zastosowanie procesorów od 4 do 40 rdzeni, mocy do min. 270W i taktowaniu CPU do min. 3.6GHz. |
| Liczba procesorów | Min. 2 procesory |
| Pamięć operacyjna | Min. 128GB RDIMM DDR4 3200 MT/s w modułach pamięci o pojemności min. 32 GB każdy.Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB.  |
| Sloty rozszerzeń | Min. 3 aktywne gniazda PCI-Express generacji 4, gniazda pełnej wysokości (full height) gotowe do obsadzenia kartami z portami zewnętrznymi, w tym min. 1 slot x16 (szybkość slotu – bus width). Serwer z możliwością rozbudowy do 8 gniazd PCI-Express generacji 4, gniazda pełnej wysokości (full height) gotowe do obsadzenia kartami z portami zewnętrznymi, w tym min. 2 sloty x16 (szybkość slotu – bus width). |
| Dysk twardy | Zatoki dyskowe gotowe do zainstalowania min. 8 dysków 3.5” typu Hot Swap, SAS/SATA/SSD. Zainstalowane min. 8 szt. dysków 8TB SAS.Zainstalowane min. 2szt. dysków SSD NVMe 480GB nie zajmujące wnęk na dyski pracujące w konfiguracji ze sprzętowym RAID 1.Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 32GB i redundancję danych RAID-1.  |
| Kontroler | Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę min. 8 napędów dyskowych SSD/SATA/SAS/NVMe. Kontroler nie zajmujący gniazd opisanych w sekcji „Sloty rozszerzeń”.Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie.Możliwość rozbudowy o kontroler z min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, min. 32 portowy obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę min. 24 napędów dyskowych SSD/SATA/SAS/NVMe. |
| Interfejsy sieciowe | Minimum 4 porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.Zainstalowana karta 2 portowa 10Gb SFP+ oparta o chipset BCM57412. |
| Karta graficzna | Zintegrowana karta graficzna |
| Porty | 5 x USB 3.0 (w tym 2 porty wewnętrzne)1x VGA 1x cyfrowy port video ( Display Port lub HDMI), bez użycia przejściówek z portu VGA lub USBMożliwość rozbudowy/rekonfiguracji o:1x port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express. |
| Zasilacz | 2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1000W klasy Titanium. |
| Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug |
| Bezpieczeństwo | Serwer wyposażony w moduł TPM 2.0 |
| Karta/moduł zarządzający | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:* monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe
* praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP
* dostęp do karty zarządzającej poprzez
	+ dedykowany port RJ45 z tyłu serwera lub
	+ przez współdzielony port zintegrowanej karty sieciowej serwera

 dostęp do karty możliwy * + z poziomu przeglądarki webowej (GUI)
	+ z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)
	+ z poziomu skryptu (XML/Perl)
	+ poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)
* wbudowane narzędzia diagnostyczne
* zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego
* obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie
* wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
* przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)
* obsługa zdalnego serwera logowania (remote syslog)
* wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów
* mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie
* funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności
* monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji
* konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
* zdalna aktualizacja oprogramowania (firmware)
* zarządzanie grupami serwerów, w tym:
	+ tworzenie i konfiguracja grup serwerów
	+ sterowanie zasilaniem (wł/wył)
	+ ograniczenie poboru mocy dla grupy (power capping)
	+ aktualizacja oprogramowania (firmware)
	+ wspólne wirtualne media dla grupy
* możliwość równoczesnej obsługi przez 6 administratorów
* autentykacja dwuskładnikowa (Kerberos)
* wsparcie dla Microsoft Active Directory
* obsługa SSL i SSH
* enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli
* wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API
* wsparcie dla Integrated Remote Console for Windows clients
* możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
* Zapewniona ochrona przed uruchomieniem nieautoryzowanego oprogramowania podczas uruchamiania serwera – Silicon Root of Trust
 |
| Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych | Microsoft Windows Server 2019, 2022Ubuntu 20.04 LTS, 22.04 LTSRed Hat Enterprise Linux (RHEL) 7.9, 8.2, 9.0SUSE Linux Enterprise Server (SLES) 12 SP5, 15 SP2VMware ESXi 7.0 U2/U3, 8.0 U1/U2 |
| System monitorowania i analizowania konfiguracji serwerów | Dostęp do systemu dla każdego serwera. Licencje dożywotnie ze wsparciem technicznym na okres zgodny z wymaganą gwarancją/wsparciem serwisowym dla serwerów.System w postaci platformy uruchomionej w chmurze i dostępnej jako usługa webowa (z przeglądarki internetowej), system niezależny od infrastruktury IT miejsca instalacji serwerów. Platforma wspierana uczeniem maszynowym i analizą predykcyjną, zapewniająca automatyczne zbieranie i analizę danych z modułów zarządzania serwerami w celu monitorowania, analizy ich pracy i porównania zachowania serwerów z danymi z referencyjnej bazy danych wszystkich podłączonych do tego systemu serwerów.System zapewniający:- scentralizowany widok parametrów monitorowanych serwerów, co najmniej: numer seryjny, stan zdrowia (Ok, Ostrzeżenie, itp), stan zasilania (Wł., Wył.), nazwa produktu (model serwera), status poszczególnych komponentów (zasilacz, pamięć, procesor, dyski, itp.);- informacje na temat stanu gwarancji serwera – co najmniej czy jest aktywna;- prezentację wersji zainstalowanego oprogramowania układowego na poszczególnych komponentach serwera;- rekomendacje odnośnie optymalizacji i poprawy wydajności serwerów, przewidywanie oraz zapobieganie problemom;- analizę danych pod kątem bezpieczeństwa serwerów np. ostrzeganie użytkownika o nieudanych próbach logowania;- prognozy pod kątem awarii poprzez ostrzeganie użytkownika o uszkodzonych komponentach.- zalecenia dotyczące eliminacji źródeł/przyczyn problemów np. wydajnościowych serwerów. |
| Oprogramowanie systemowe | Zamawiający wymaga, aby dostarczony serwer posiadał zainstalowane oprogramowanie systemowe w najnowszej aktualnej wersji, nieograniczonej czasowo wraz z licencją dostępową dla 80 urządzeń oraz dla 5 użytkowników korzystających z usług pulpitu zdalnego. Zamawiający wymaga, aby dostawa obejmowała licencje dla użytkowników umożliwiające działanie licencji zgodnie z wymaganiami licencyjnymi.  |
| Wsparcie techniczne | Minimum 3-letnia gwarancja producenta w miejscu instalacji.Czas reakcji 2h w standardowe dni robocze w godzinach od 9:00 do 17:00. Przybycie serwisu do miejsca instalacji w ciągu następnego dnia roboczego od zgłoszenia usterki. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera.  |
| Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.Deklaracja zgodności CE. |

# 2. WARTOŚCI NIEMATERIALNE I PRAWNE

## 2.1 Red Hat Enterprise Linux Server lub równoważny

* Wersja: Cyfrowa / do pobrania
* Licencja: na serwer
* Czas trwania: 3 lata
* Wsparcie: 24x7

System Operacyjny

* RHEL 7 lub nowszy (dla równoważnych dystrybucji, wersje kompatybilne z RHEL 7 lub nowszym)

Jądro Systemu

* Wersja jądra dostarczona przez Red Hat lub równoważna

Menedżer Pakietów

* Yum (Yellowdog Updater Modified) dla RHEL 7 i starszych
* DNF (Dandified Yum) dla RHEL 8 i nowszych

Środowisko Graficzne (opcjonalnie)

* GNOME, KDE lub inne środowiska graficzne wspierane przez dystrybucję

Dodatkowe Wymagania i Zależności

Bezpieczeństwo

* Selinux (Security-Enhanced Linux) w trybie enforcing dla zwiększonego bezpieczeństwa
* Aktualne oprogramowanie antywirusowe i antymalware

Zarządzanie Systemem

* Red Hat Satellite Server (opcjonalnie, dla centralnego zarządzania)
* Cockpit jako webowy interfejs do zarządzania serwerem

Sieć i Usługi

* Dostęp do repozytoriów Red Hat lub równoważnych (np. EPEL)
* Konfiguracja zapory sieciowej (firewall) i zabezpieczeń sieciowych (np. iptables, firewalld)

Narzędzia do Zarządzania i Monitorowania

* Systemy monitorowania takie jak Nagios, Zabbix, Prometheus
* Narzędzia do zarządzania logami, np. Logrotate, ELK Stack (Elasticsearch, Logstash, Kibana)

Wirtualizacja

* Obsługa wirtualizacji z wykorzystaniem KVM (Kernel-based Virtual Machine), Xen, lub innego kompatybilnego hypervisora

## 2.2 Windows Server 2022 Standard lub równoważny – 12 szt. (1 komplet)

|  |  |
| --- | --- |
| Producent  | Microsoft lub równoważny  |
| Zawartość pakietu  | Microsoft Windows Server Standard 2022 lub równoważny  |
| Rodzaj licencji  | nowa licencja  |
| Okres licencji  | wieczysta  |
| Jednostka licencjonowania  | 24 rdzenie procesora  |
| Wersja językowa  | polska  |
| Model  | Microsoft Windows Server Standard 2022 lub równoważny  |

## 2.3 Windows Server 2022 External Connector lub równoważny – 1 szt.

|  |  |
| --- | --- |
| Producent  | Microsoft lub równoważny  |
| Wersja  | 2022  |
| Wersja językowa  | polska  |

## 2.4 Certyfikaty serwerowe

2.4.1. **Wymagania Techniczne**

**Klucz prywatny:**

1. **Długość klucza:** Minimum 2048 bitów (zalecane 4096 bitów dla większego bezpieczeństwa).
2. **Algorytm:** RSA, ECDSA, lub inne bezpieczne algorytmy klucza publicznego.

**Certyfikat:**

* **Format certyfikatu:** X.509.
* **Format pliku:** PEM (.pem), DER (.der), PKCS#12 (.p12, .pfx).

**Podpis cyfrowy:**

* Wymagane jest, aby certyfikaty były podpisane przez zaufane Urzędy Certyfikacji (CA).
* Algorytm podpisu: SHA-256 lub nowszy.

2.4.2. **Wymagania Urzędów Certyfikacji (CA)**

**Weryfikacja domeny:**

* CA musi zweryfikować, że żądający certyfikatu jest właścicielem lub ma prawo do używania domeny. Może to być wykonane poprzez:
	+ Email do administratora domeny.
	+ Publikację specyficznego kodu na stronie internetowej domeny.

Aktualizację DNS.

**Weryfikacja tożsamości:**

Dla certyfikatów typu OV (Organization Validated) i EV (Extended Validation), CA wymaga dodatkowej weryfikacji organizacji, w tym dokumentów rejestracyjnych firmy, dowodu tożsamości osoby odpowiedzialnej itp.

## 2.5 Oprogramowanie antywirusowe z wbudowanym systemem EDR – 1 szt.

2.5.1 Wymagania minimalne:

**\* Licencja 3 letnia dla 80 użytkowników**

**Administracja zdalna w chmurze**

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. 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.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

2.5.2 Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
16. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
17. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
18. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
19. 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,
20. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
21. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z:
22. zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
23. 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.
24. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
25. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
26. Rozwiązanie musi posiadać funkcjonalność skanera UFEI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
27. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
28. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
29. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
30. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
31. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
32. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
33. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
34. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
35. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
36. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
37. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
38. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
39. 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.

2.5.3 Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz
2. Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu
3. Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
4. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
5. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
6. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
7. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
8. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
9. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
10. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

**Dodatkowe wymagania dla ochrony serwerów Windows:**

1. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
2. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
3. Rozwiązanie musi posiadać funkcjonalność skanera UFEI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
4. Rozwiązanie musi zapewniać 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.
5. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
6. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
7. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
8. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

2.5.4. Dodatkowe wymagania dla ochrony serwerów Linux:

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów.

Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

2.5.5 Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UFEI.

2.5.6 Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. 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.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
13. Czysty,
14. Podejrzany,
15. Bardzo podejrzany,
16. Szkodliwy.
17. 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.
18. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
19. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

2.5.8 Moduł XDR

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. 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.
10. 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.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. 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.
13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
14. 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.
15. 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.
16. Konsola administracyjna musi mieć możliwość tagowania obiektów.
17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell

## 2.6 Oprogramowanie w zakresie cyberbezpieczeństwa 1- szt.

|  |  |
| --- | --- |
| LP | Wymaganie |
| 1 | Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji |
| a | Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012 |
| b | Vmware vSphere min. w wersjach v5.5-7.0.3 |
| c | Nutanix AHV 5.15, 5.20 (LTS) |
| d  | Maszyny fizyczne: Windows Server 2022, 2019, 2016, 2012R2, 2012 |
| e | Microsoft 365 (Exchange online, One Drive for Business, Sharepoint) |
| 2 | Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V |
| 3 | Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia: |
| a | na serwerze Windows lub Linux  |
| b | jako maszyna wirtualna Vmware |
| c | jako maszyna wirtualna Amazon |
| d  | na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital |
| 4 | Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS |
| 5 | Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania |
| 6.  | Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).  |
| II | Licencjonowanie |
| 1 | Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności |
| 2 | Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 6 gniazd procesorów w obrębie środowiska |
| 3 | W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 1 roku wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania |
| 4 | W ramach dostawy wymagane jest dostarczenie licencji na ochronę 2 gniazd procesorów w hostach Vmware lub Hyper-V |
| 5 | Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska |
| III | Ochrona danych |
| 1 | Oprogramowanie musi posiadać funkcje backupu i replikacji: |
| a | Backup maszyn wirtualnych Vmware |
| b | Replikacja maszyn wirtualnych Vmware (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu |
| c | Backup maszyn wirtualnych Hyper-V |
| d  | Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu |
| e | Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych |
| f | Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie |
| g | Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu |
| h | Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym |
| i | Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem |
| j | Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania |
| IV | Optymalizacja wykorzystania miejsca na dane |
| 1 | Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych: |
| a | Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane |
| b | Kompresja backupu, w tym konfigurowalny stopień kompresji |
| c | Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne |
| V | Spójność danych |
| 1 | Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:  |
| a | Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux  |
| b | Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu  |
| c | Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji:  |
|  | Microsoft Exchange 2013, 2016, 2019 |
|  | Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022 |
| d  | Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki |
| e | Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V |
| f | Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania |
| g | Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji |
| VI | Przywracanie danych |
| 1 | Oprogramowanie musi posiadać poniższe funkcje: |
| a | Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji |
| b | Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej) |
| c | Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej) |
| d  | Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu): |
|  | Microsoft Exchange  |
|  | Active Directory |
|  | MS SQL |
| e | Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.  |
| VII | Wydajność |
| 1 | Oprogramowanie do backupu musi pozwalać na: |
| a | Tworzenie backupu I replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT |
| b | Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych |
| c | Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN  |
| d  | Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci |
| VIII | Zarządzanie |
| 1 | Oprogramowanie musi pozwalać na następujące formy zarządzania: |
| a | Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych  |
| b | Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej |
| c | Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania |
| d  | Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.  |
| e | Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji |

# 3. Instalacja i konfiguracja urządzeń

W ramach zamówienia zostanie dostarczony opisany powyżej sprzęt i oprogramowanie oraz wykonane następujące prace:

1. Sprzęt zostanie rozpakowany, podłączony oraz zostanie wykonana podstawowa konfiguracja.
2. Serwer musi zostać zainstalowany w szafie RACK.
3. Instalacja i konfiguracja systemu wirtualizacyjnego.
4. Instalacja i konfiguracja maszyn wirtualnych na podstawie dostarczonych przez Zamawiającego parametrów.
5. Instalacja oprogramowania do wykonywania backupu.
6. Integracja systemu backupu z platformą wirtualizacyjną.
7. Przeprowadzenie testów backupu i odtwarzania.
8. Instalacja i konfiguracja oprogramowania antywirusowego.
9. Wykonawca przygotuje niezbędną dokumentację w zakresie dokumentacji powdrożeniowej zawierającej opis konfigurowanych opcji wdrożonego środowiska serwerowego.
10. Wykonawca zapewni 8h supportu powdrożeniowego z zakresu dostarczonych rozwiązań. W ramach udzielonego wsparcia technicznego Zamawiający będzie miał możliwość skorzystania z konsultacji telefonicznych/email oraz zdalnej pomocy. Wsparcie techniczne będzie świadczone przez inżyniera posiadającego wiedzę i doświadczenie z zakresu dostarczonych rozwiązań.