**Zał. 1 – opis przedmiotu zamówienia**

Zamówienie – kompleksowe i całościowe dostarczenie rozwiązania IT w celu polepszenia cyberbezpieczeństwa.

W ramach tego rozwiązania dostarczone zostanie rozwiązanie IT w postaci: systemu zabezpieczenia danych, zarządzalne urządzenia sieciowe, serwerów fizycznych, macierzy dyskowej, serwerowego systemu operacyjnego i oprogramowania bezpieczeństwa oraz zasilania awaryjnego.

Celem zamówienia jest zwiększenie poziomu cyberbezpieczeństwa ww. podmiotów poprzez wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych. Celem jest wdrożenia mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni.

W wyniku podjętych działań przyczyniających się do sprawnego i bezpiecznego działania systemów informatycznych, podniesie się poziom cyberbezpieczeństwa.

W celu wzmocnienia odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informatycznych konieczny jest zakup sprzętu, oprogramowania i usług informatycznych w obszarze cyberbezpieczeństwa jako kompleksowego i efektywnego rozwiązania.

Skutkiem realizacji będzie skuteczne zabezpieczenie systemów informatycznych przed cyberprzestępczością w kontekście: ochrony danych osobowych (RODO), potencjalnej utraty danych, ujawnienia wrażliwych danych osobom nieuprawnionym albo umożliwienia atakującym zniszczenia dokumentów lub danych, co zapewni ciągłość pracy oraz zwiększy poczucie bezpieczeństwa.

**Przedmiot obejmuje kompleksowe rozwiązanie:**

1. System zabezpieczeń danych - Backup środowiska wraz z oprogramowaniem i usługą składającą się z: projekt, wdrożenie, troubleshooting, wsparcie DR w przypadku konieczności odtwarzania środowiska po ataku.
2. Zarządzalne urządzenia sieciowe wraz z wdrożeniem– 3 szt. switch.
3. Serwer fizyczny wraz z wdrożeniem– 1 szt.
4. Macierze dyskowe wraz z wdrożeniem– 1 szt.
5. Serwerowe systemy operacyjne i oprogramowanie bezpieczeństwa – 4 szt. Serwerowy system operacyjny, 1 szt. oprogramowanie do zarządzania infrastrukturą IT, 1 szt. przedłużenie licencji oprogramowania dla FortiGate 60F UTP, 50 szt. licencji oprogramowanie antywirusowe.
6. Zasilanie awaryjne wraz z wdrożeniem– 1 szt. UPS 5000VA

**[System zabezpieczenia danych]**

System zabezpieczeń danych: Backup środowiska wraz z oprogramowaniem i usługą składającą się z: projekt, wdrożenie, troubleshooting, wsparcie DR w przypadku konieczności odtwarzania środowiska po ataku. Wraz z tym zostanie dostarczona 1 szt. urządzenia Appliance wraz z licencjami o łącznej pojemności środowiska danych backupowanych do 5TB, złożonego z systemu Windows 10/11/2016/2022 oraz Linux Ubuntu, CentOS środowisko mieszane – maszyny fizyczne oraz Wirtualne VMWARE oraz Microsoft Hyper-V.

System zabezpieczeń danych:

Backup środowiska wraz z oprogramowaniem i usługą składającą się z: projektu, wdrożenia, troubleshooting, wsparcia DR w przypadku konieczności odtwarzania środowiska po ataku.

1 szt. system backup zbudowany w oparciu o urządzenie Appliance łączące funkcję repozytorium, serwerów zarządzających i zabezpieczających dane, wraz z licencjami o łącznej pojemności danych backupowanych do 5TB

Minimalne wymaganie dotyczące jednej sztuki systemu zabezpieczeń danych.

W ramach postępowania należy dostarczyć sprzęt, licencje i usługi konieczne dla zbudowania i utrzymania systemu.

Wymagania dla usług:

Minimalne wymaganie dotyczące jednej sztuki systemu zabezpieczeń danych.

1. Zarządzanie i magazyny

System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.

2. Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe:

a. Obudowa rack rozmiar: maksymalnie 2U.

b. Procesor:

wielordzeniowy procesor o parametrach dedykowanych przez producenta rozwiązania

c. Pamięć RAM:

min. 16 GB DDR4.

d. Przestrzeń dostępna na przechowywanie danych:

min. 24 TB po RAID5

e. Osobne dyski SSD M.2 nVME działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego,

f. Redundantne zasilanie,

g. Minimum 1 interfejs Ethernet 1Gb, oraz 1 interfejs Sfp+ 10Gb, wraz z zestawem dwóch wkładek o prędkości minimum 10Gb, oraz patchcordem 3metry

h. Gwarancja NBD on-premise obowiązuje przez okres min. 24 miesiące

3. Produkt dostępny w polskiej wersji językowej.

4. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej

5. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków

6. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów

7. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych

8. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT

9. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft

10. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe

11. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).

12. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).

13. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.

14. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.

15. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.

16. Rozwiązanie w warstwie sprzętowej powinno bazować na standardowych komponentach architektury x86

17. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.

18. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.

19. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.

20. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.

21. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.

22. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych

23. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.

24. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.

25. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).

26. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.

27. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.

28. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,

29. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.

30. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.

31. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).

32. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.

33. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.

34. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych

35. Proces deduplikacji nie może posiadać pojedynczego punktu awarii

36. Proces deduplikacji realizowany jest blokiem o stałej wielkości.

37. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.

38. Kompresja kopii zapasowych, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.

39. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.

40. System musi pozwalać na automatyczne aktualizacje oprogramowania.

41. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.

42. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS w celu ich zabezpieczenia.

43. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.

44. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.

45. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.

46. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.

47. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.

48. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.

49. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.

50. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.

51. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.

52. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

53. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych: G-F-S, Forever incremental,

54. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).

55. Możliwość składowania utworzonych kopii zapasowych na magazynach zgodnych z S3.

56. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, nfs, iscsi, katalog lokalny

57. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).

58. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.

59. Możliwość generowania raportów dobowych w oparciu o harmonogram

60. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter musi być zlokalizowane na terenie Polski)

61. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)

62. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.

63. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)

2. Środowiska fizyczne i bazy danych

1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.

2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.

3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.

4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt.

5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.

6. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.

7. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.

8. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.

9. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.

10. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).

11. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.

12. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

3. Środowiska wirtualne

1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.

2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.

3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.

4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.

5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.

6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).

7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.

8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.

5. Licencjonowanie i wsparcie techniczne

1. Wszystkie linie supportu muszą być obsługiwane w języku polskim.

2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.

3. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)

4. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.

5. W ramach wsparcia technicznego Zamawiający musi mieć dostęp do tzw. Dedicated Customer Success Managera, tj. osoby po stronie Dostawcy dedykowanej do obsługi zgłoszeń technicznych, doraźnej pomocy i bieżącej pomocy w utrzymania infrastruktury Zamawiającego.

6. W ramach dokumentacji posprzedażowej Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do Dedicated Customer Success Managera.

7. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych.

8. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu, a system zachowuje pełną funkcjonalność

9. Dostęp do wsparcia technicznego producenta obowiązuje analogicznie do czasu trwania gwarancji na dostarczone urządzenie

10. Licencje powinny umożliwiać replikację na własne zasoby.

11. Licencje powinny umożliwiać korzystanie z przestrzeni chmurowej min. 4,8TB dostarczonej bezpośrednio przed producenta przez cały okres trwania gwarancji NBD na warstwę sprzętową.

6. Anty-ransomware i bezpieczeństwo

1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").

2. System powinien umożliwiać wykorzystanie wbudowanego menadżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System

3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.

**[Zarządzalne urządzenie sieciowe]**

**3 szt. Switch**

Wymiana obecnych przełączników na nowoczesne przełączniki zarządzane, które umożliwią bezpieczną separację sieci. Wraz z dostarczonymi przełącznikami wykonawca wdroży separację sieci, rozgraniczając stacje komputerowe, urządzenia drukujące oraz serwery, zachowując przy tym niezbędną ciągłość działania jednostki. W ramach wdrożenia skonfigurowane zostanie również urządzenie Fortigate 60F w celu nadzoru nad ruchem pomiędzy wydzielonymi sieciami.

Sieć Zleceniobiorcy złożona jest z około 60 urządzeń końcowych.

**1 szt. Switch 48 port**

Minimalne wymaganie dotyczące jednej sztuki przełącznika zarządzalnego dostępowego 48 port.

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack, oraz 4zestawy, czyli 8 wkładek światłowodowych Hot-Plug SFP+ Min. prędkość: 10 GB/s wraz z 4x patchcord odługości minimum 10metrów. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.

2. Wymagane parametry fizyczne:

Warstwa przełączania L2/L3

Porty: 48 x 10/100/1000Base-T + minimum 4 x 10 Gigabit SFP+, min. 1 x USB-C konsola

Szybkość przesyłania dalej (pakiety 64-bit): min. 130 Mpps

Zdolność przełączania min: 176 Gb/s

Grupy agregacji łącza: min. 8

Agregacja łączy (portów): min. 8

Możliwość łączenia w stos

Możliwość tworzenia VLAN

Identyfikatory sieci VLAN: min. 4093

Interfejsy IPv4: min. 128

Reguły ACL: min. 1024

Kolejki priorytetów: min. 8

Rozmiar bufora pakietu: min. 1.5 MB

Wielkość tablicy adresów MAC: min. 16000 wpisów

Obsługiwane ramki Jumbo: min. 9000 bajtów

Maks. ilość części w wieży: min.8

Protokół routingu: RIP-2, IGMPv2, IGMP, statyczne trasowanie IP, IGMPv3, policy-based routing (PBR), MLDv2, MLD, CIDR, MSTP, RSTP, STP, Bounjour

Obsługa: SNMP, RMON, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH, SSH-2, CLI, SCP, ICMP, DHCP, RADIUS, Syslog

RAM: min. 1 GB DDR4 SDRAM

Pamięć fleszowa: min. 512 MB

Gwarancja – minimum 2 lata

**2 szt. Switch 16 port**

W ramach postępowania dostarczone zostaną 2 sztuki urządzenia switch 16port

Minimalne wymaganie dotyczące 1 x przełącznika zarządzalnego dostępowego 16 port.

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack oraz 8 wkładek światłowodowych Hot-Plug SFP+ Min. prędkość: 10 GB/s wraz z 8x patchcord długości minimum 1metr

System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.

2. Wymagane parametry fizyczne:

Warstwa przełączania L2/L3

Porty: 16 x 10Gb w tym minimum 8x10GbE oraz minimum 8x10Gb SFP+, min. 1 x USB-C konsola

Szybkość przesyłania dalej (pakiety 64-bit): min. 238 Mpps

Zdolność przełączania min: 320Gb/s

Grupy agregacji łącza: min. 8

Agregacja łączy (portów): min. 8

Możliwość łączenia w stos

Możliwość tworzenia VLAN

Identyfikatory sieci VLAN: min. 4093

Interfejsy IPv4: min. 128

Reguły ACL: min. 1024

Kolejki priorytetów: min. 8

Rozmiar bufora pakietu: min. 3 MB

Wielkość tablicy adresów MAC: min. 16000 wpisów

Obsługiwane ramki Jumbo: min. 9000 bajtów

Maks. ilość części w wieży: min.8

Protokół routingu: RIP-2, IGMPv2, IGMP, statyczne trasowanie IP, IGMPv3, policy-based routing (PBR), MLDv2, MLD, CIDR, MSTP, RSTP, STP, Bounjour

Obsługa: SNMP, RMON, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH, SSH-2, CLI, SCP, ICMP, DHCP, RADIUS, Syslog

RAM: min. 1 GB DDR4 SDRAM

Pamięć fleszowa: min. 512 MB

Gwarancja – minimum 2 lata

**[Serwer fizyczny]**

1 szt. serwer fizyczny

Minimalne wymaganie dotyczące jednej sztuki serwera.

Wykonawca winien opisać/podać oferowane parametry:

1. Informacje ogólne

1.1 Urządzenie musi być fabrycznie nowe i nieużywane przed dniem dostarczenia do siedziby Zamawiającego, z wyłączeniem użycia niezbędnego dla przeprowadzenia testu ich poprawnej pracy.

2. Obudowa

2.1 Obudowa typu RACK o wysokości maksymalnej 1U

2.2 Możliwość instalacji min. 8 dysków 2,5” Hot-Plug

2.3 Obudowa wyposażona w panel diagnostyczny lub sygnalizację LED umieszczoną na froncie obudowy informująca o stanie serwera.

2.4 Musi być wyposażona w przednią ramkę, zamykaną na klucz, chroniącą dyski przed nieuprawnionym wyjęciem.

2.5 Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Ramię do zarządzania przewodami.

3. Płyta główna

3.1 Płyta główna z możliwością zainstalowania minimum dwóch procesorów

4. Procesor

4.1 Dwa procesory wielordzeniowe osiągające w teście PassMark CPU Mark wynik min. 44.500 pkt według danych ze strony https://www.cpubenchmark.net/multi\_cpu.html dla konfiguracji wieloprocesorowej

5. Pamięć RAM

5.1 Zainstalowana pamięć RAM minimum 256 GB RDIMM lub LRDIMM.

5.2 Rozmiar pojedynczej kości pamięci RAM minimum 32GB

5.3 Możliwość rozbudowy do minimum 1 TB.

6. Pamięć masowa

6.1 Minimum 3 dysków 960GB SSD typu HotPlug

6.2 Możliwość instalacji dysków twardych SATA, SAS, SSD.

6.3 Możliwość instalacji modułu dedykowanego dla hypervisora wirtualizacyjnego.

7. Kontroler

7.1 Sprzętowy kontroler dyskowy RAID obsługujący poziomy 0, 1, 5, 6, 10, 50, 60, wyposażony w pamięć cache o pojemności min. 8GB oraz podtrzymanie bateryjne. Wsparcie dla dysków samoszyfrujących.

8. Karta graficzna

8.1 Zintegrowana karta graficzna o rozdzielczości minimum 1920x1200

9. Wbudowane porty

9.1 Minimum 2 porty USB wersji 3.0 lub nowszej.

9.2 1 port USB na przednim panelu obudowy

9.3 Minimum 1 port VGA.

10. Interfejsy sieciowe

10.1 Sumarycznie minimum cztery interfejsy sieciowe minimum 2x 10GB SFP+, minimum 2x 10 GbE BASE-T zapewnione przez minimum 2 karty sieciowe (Po 2 interfejsy na jednej karcie sieciowej).

10.2 Jeden interfejs 1Gb w standardzie Base-T do zarządzania serwerem.

11. Zasilanie

11.1 Redundantne zasilacze Hot Plug, każdy klasy Titanium, pracujące w sieci 230V 50/60Hz prądu zmiennego.

12. Wentylatory

12.1 Redundantne wentylatory typu Hot-Plug.

13. Bezpieczeństwo

13.1 Zintegrowany z płytą główną moduł TPM 2.0.

13.2 Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.

13.3 Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

13.4 BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła

13.5 Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.

13.6 Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).

14. Zarządzanie

14.1 Moduł umożliwiający zdalne zarządzanie serwerem.

14.2 Oprogramowanie do zdalnego zarządzania serwerem, zapewniające minimum: monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.), monitorowanie w czasie rzeczywistym poboru prądu przez serwer, zbieranie logów błędów hardware, przechwycenie wirtualnej konsoli wraz z dostępem do ekranu, myszy i klawiatury, montowanie wirtualnych napędów, wysyłanie zawiadomień droga mailową i poprzez SNMP. Jeśli do powyższej funkcjonalności wymagane są dodatkowe licencje, zostaną one dostarczone

15. Certyfikaty i Deklaracje

15.1 Deklaracja zgodności UE (Certyfikat CE).

15.2 Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.

15.3 Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.

16. Wsparcie serwisowe

16.1 Urządzenie musi być wyprodukowane nie wcześniej niż w 2024 roku i pochodzić z legalnego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub właściwego partnera serwisowego lub wykonawcy z akredytacją producenta.

16.2 Urządzenie musi zostać objęte okresem gwarancji 36 miesięcy w trybie NBD onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki.

16.3 Urządzenie przystosowane do napraw w miejscu instalacji.

16.4 Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet.

16.5 Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.

16.6 Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.

16.7 Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.

16.8 Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

**[Macierz dyskowa]**

1 szt. macierz dyskowa

Minimalne wymaganie dotyczące jednej sztuki macierzy.

Wykonawca winien opisać/podać oferowane parametry

1. Obudowa

1.1 System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''

2. Pojemność:

2.1 System musi zostać dostarczony w konfiguracji zawierającej minimum:

2.1.1 8 dysków 3,8 TB SSD

2.2 System musi posiadać możliwość rozbudowy o kolejne dyski

2.3 System musi wspierać dyski:

2.3.1 SSD: 800GB do 7600GB

2.4 W przypadku klastrowania kontrolerów macierzy, system musi działać pod kontrolą jednego systemu operacyjnego od jednego producenta, niedopuszczalne jest zestawienie systemu klastrowego poprzez wykorzystanie serwerów pośredniczących i oprogramowania dodatkowego.

2.5 Dla rozwiązań wykorzystujących klastrowanie (scale-out) musi być możliwość rozbudowy rozwiązania do co najmniej 10 kontrolerów w klastrze.

2.6 Macierz wyposażona w minimum dwa zasilacze

3. Kontroler

3.1 Dwa kontrolery wyposażone w przynajmniej 32GB cache każdy.

3.2 Procesory macierzy powinny być wykonane w technologii wielordzeniowej z przynajmniej 12 rdzeniami na każdy kontroler dla procesorów X86. Dla innych rodzajów procesorów min 64 rdzenie.

3.3 W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub poprzez zrzut na pamięć nieulotną

3.4 Macierz musi pozwalać na poszerzenie pamięci Cache za pomocą dysków SSD.

4. Interfejsy

4.1 Oferowana macierz musi posiadać minimum

4.1.1 4 porty 10GbE SFP+

4.1.2 2 porty 1Gb do zarządzania

5. RAID

5.1 System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii minimum dwóch dysków w grupie RAID

6. Kopie Migawkowe

6.1 Macierz musi być wyposażona w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności macierzy +/-5%

6.2 Zamawiający dopuszcza rozwiązanie, które ma wpływ na wydajność przy stosowaniu kopii migawkowych przy zapisie, przy założeniu zaoferowania całej pojemności na dyskach SSD/Flash/NVME.

7. Obsługiwane protokoły

7.1 Macierz musi obsługiwać jednocześnie protokoły FC, iSCSi, CIFS i NFS, S3 (macierz obiektowa) - jeśli wymagane są licencje zamawiający wymaga dostarczenia ich wraz z macierzą.

8. Inne wymagania

8.1 Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Win 2018 i nowsze, Linux, Vmware

8.2 Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie

8.3 Macierz musi posiadać funkcjonalność priorytetyzacji zadań.

8.4 Macierz musi posiadać funkcjonalność kompresji danych w trybie in-line oraz off-line na każdym rodzaju danych.

8.5 Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych którą można stosować na macierzy/danych produkcyjnej dla wszystkich rodzajów danych. Jeżeli oferowane rozwiązanie nie posiada funkcjonalności deduplikacji danych, zamawiający wymaga dostarczenia 4-krotności przestrzeni wyspecyfikowanej.

8.6 Macierz musi posiadać funkcjonalność replikacji synchronicznej i asynchronicznej pomiędzy macierzami tego samego producenta. Funkcjonalność replikacji danych musi być natywnym narzędziem macierzy.

8.7 System musi posiadać specjalny moduł do zabezpieczenia przez atakiem Ransomware w szczególności:

8.7.1 musi informować administratora w przypadku niestandardowego zachowania systemu oraz danych

8.7.2 wykonywać prewencyjną kopię migawkową „snapshot” w przypadku zagrożenia atakiem ransomware

8.7.3 monitorować niestandardowe zachowanie użytkowników serwera plików

8.8 Macierz musi posiadać zaimplementowaną funkcjonalność WORM. Jeżeli rozwiązanie wymaga do tego licencji zamawiający wymaga jej dostarczenia.

8.9 W celach bezpieczeństwa macierz musi posiadać funkcjonalność wieloetapowej akceptacji wybranych operacji tj. operacje takie jak: Skasowanie LUN/Wolumeny, skasowanie Snapshotu, wyłączenie replikacji. System musi pozwalać by wykonanie w/w operacji było akceptowane przez przynajmniej dwóch administratorów w celu zwiększenia bezpieczeństwa i uniknięcia błędów ludzkich.

8.10 Macierz musi posiadać funkcjonalność wykonania wirtualnych klonów, które nie wymagają kopiowania bloków danych.

9. Gwarancja 24 miesiące

9.1 serwis gwarancyjny, w tym producenta z dostawą elementów w na następny dzień roboczy

**[Serwerowe systemy operacyjne i oprogramowanie bezpieczeństwa]**

**4 szt. Serwerowy system operacyjny.**

Zamawiający zamierza zakupić system operacyjny Microsoft Windows Server 2025 Standard Edition 16-core.

Zamawiający dopuszcza zaoferowania oprogramowania równoważnego, poprzez które należy rozumieć oferowane oprogramowanie o parametrach nie gorszych od opisanych jako wymagane, umożliwiające wykorzystanie urządzeń, w takim samym zakresie i stopniu skomplikowania, co oprogramowanie określone w opisie przedmiotu zamówienia.

Oprogramowanie Systemu Operacyjnego (OSO) musi posiadać następujące cechy, funkcje i minimalne parametry:

1. Współpraca z procesorami o architekturze x86-64.

2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.

3. Obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing. i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu.

4. Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie minimum Microsoft Windows Server 2016.

5. Licencja musi uprawniać do uruchamiania wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

6. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor. przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

8. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów. w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

9. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.

10. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

11. Graficzny interfejs użytkownika. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.

12. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

13. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

14. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).

15. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

15.1 Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.

15.2 Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach,

15.3 Pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe.

15.4 Zdalna dystrybucja oprogramowania na stacje robocze.

15.5 Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.

15.6 PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

15.6.1 Dystrybucję certyfikatów poprzez http,

15.6.2 Konsolidację CA dla wielu lasów domeny,

15.6.3 Automatyczne rejestrowania certyfikatów pomiędzy rożnymi lasami domen.

15.7 Szyfrowanie plików i folderów.

15.8 Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

15.9 Serwis udostępniania stron WWW.

15.10 Wsparcie dla protokołu IP w wersji 6 (IPv6).

15.11 Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.

16. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.

17. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).

18. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

19. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF15.6.; W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania.

**1 szt. Oprogramowanie do zarządzania infrastrukturą IT**

Zamawiający wykorzystuje obecnie oprogramowanie Axence Nvision 13 moduły Network, Inventory, Users, Dataguard. Przedmiotem zamówienia jest rozszerzenie licencji z 40 do 50 stanowisk, przedłużenie posiadanej licencji oraz aktualizacja do najnowszej wersji oprogramowania.

Okres do 30 czerwca 2026 r.

Zamawiający dopuszcza również rozwiązanie równoważne spełniające minimum poniższe wymagania:

Wymagania ogólne

1. Obsługa min. 50 komputerów i serwerów
2. Obsługa min. 50 użytkowników
3. Nielimitowana ilość pozostałych urządzań
4. System zgodny z RODO w zakresie przechowywania oraz udostępniania danych osobowych
5. Działania administratorów są logowane oznacza to, że program posiada dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog
6. Oprogramowanie instalowane na serwerze Zamawiającego
7. Wszystkie niezbędne programy do działania systemu dostarczone w ramach niniejszej licencji
8. Licencja , wsparcie i gwarancja do 30 czerwca 2026 r., po upływie terminu wsparcia technicznego oprogramowanie pozostaje w pełni funkcjonalne

"Komunikacja pomiędzy Serwerem, komputerami a Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu

Monitorowanie infrastruktury

1. Monitorowanie komputerów pod kontrolą systemów operacyjnych ( Windows, Linux, Mac)
2. Monitorowanie serwerów pod kontrolą systemów operacyjnych (Windows, Linux)
3. Monitorowanie routerów, przełączników, urządzeń VoIP, UTM, firewall
4. Monitorowanie serwerów WWW i adresów URL
5. Monitorowanie czasu ładowania strony oraz zmian treści na stronach WWW oraz statusu protokołu HTTPS
6. Wykrywania urządzeń w sieci poprzez skanowanie
7. Wykrywanie serwisów ( TCP/IP, HTTP, POP, SMTP, FTP)
8. Monitorowanie routerów i przełączników wg ruchu sieciowego, zmian stanu interfejsów sieciowych, podłączonych stacji roboczych
9. Monitorowanie serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
10. Monitorowanie wydajności systemów Windows ( obciążenie CPU, pamięci , zajętość dysków)
11. Monitorowanie czasu pracy ( godzina rozpoczęcia, godzina zakończenia, czas pracy)

DLP

1. Monitorowanie operacji na plikach i katalogach na dysku systemowym
2. Zarzadzanie prawami dostępu
3. Monitorowanie wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość ""grupowania"" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
4. Blokowanie urządzeń i nośników danych.
5. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD
6. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
7. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością
8. ograniczenia alarmów tylko do nośników niezaufanych.
9. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.
10. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
11. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków
12. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
13. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
14. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
15. Podłączenie/odłączenie urządzenia przenośnego.

Zasoby

1. Monitorowanie szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów,
2. Monitorowanie zainstalowanych aplikacjach oraz aktualizacjach Windows
3. Wysyłanie informacji w przypadku w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu, zmian konfiguracji
4. Automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
5. Tworzenie listy plików użytkowników z określonym rozszerzeniem znalezionych na stacjach roboczych oraz ich zdalne usuwanie
6. Wskazania osób uprawnionych do użycia zasobów
7. Tworzenie listy aplikacji bezpiecznych do samodzielnego instalowania przez użytkowników
8. Zarządzanie posiadanymi licencjami - raport zgodności – SAM

Użytkownicy

1. Monitorowanie wiadomości e-mail - w cenu wykrycia phishingu
2. Blokowanie uruchamianych aplikacji
3. Raporty z wydruków - koszty
4. Blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
5. Integracja z Active Directory
6. Obsługa zgłoszeń serwisowych
7. Obsługa i zgłaszanie nadawania uprawnień
8. Zdalny dostęp do komuterów z możliwością blokowania klawiatury i myszki
9. Tworzenie listy kontaktów w organizacji

Zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami)

**1 szt. Przedłużenie licencji oprogramowania dla FortiGate 60F UTP**

Zamawiający wykorzystuje obecnie oprogramowanie FortiGate 60F UTP SN: T60FTK22096960, przedmiotem zamówienia jest przedłużenie posiadanej licencji na moduły IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, FortiCare Premium

Okres do 30 czerwca 2026 r.

**50 szt. Licencja ESET PROTECT** licencja nr 33B-DB2-B5M

Minimalne wymaganie:

Zamawiający wykorzystuje obecnie oprogramowanie ESET Endpoint Security dla 45 stacji. Należy dostarczyć licencje pozwalające rozszerzyć funkcjonalność posiadanego rozwiązania łącznie do 50 licencji dla użytkowników lub serwerów, oraz przedłużyć ważność licencji do 30 czerwca 2026 r.

Wymagane jest zarządzanie dostarczonym rozwiązaniem z posiadanej przez Zamawiającego konsoli administracyjnej ESET

W przypadku zaoferowania rozwiązania równoważnego Dostawca zobowiązany jest do dostarczenia: rozwiązania równoważnego dla wszystkich 50 użytkowników/końcówek/serwerów wraz z wdrożeniem, wymianą (odinstalowaniem ESET i zainstalowaniem nowego oprogramowania) na końcówkach/serwerach oraz certyfikowanym przez producenta szkoleniem dla administratora oraz szkoleniem dla użytkowników (może być selflearning).

Okres do 30 czerwca 2026 r.

Wykonawca dostarczy dokumenty licencyjne, warunki licencjonowania oraz klucze licencyjne i instrukcje instalacji do oprogramowania.

**Kryteria równoważności**

Oprogramowanie zaoferowane przez wykonawcę musi posiadać funkcjonalności opisane poniżej. Zamawiający dopuszcza oprogramowanie oferujące rozwiązania bardziej rozbudowane aniżeli te wskazane na poniższej liście przedstawiającej i opisującej kryteria równoważności. Dostarczone oprogramowanie musi być w pełni kompatybilne z wykorzystywanymi przez zamawiającego urządzeniami oraz posiadanym oprogramowaniem

**Kryteria równoważności (wymagane funkcjonalności):**

1. Dostarczona na oprogramowanie licencja musi umożliwiać co najmniej:
	1. Dostęp do subskrypcji aktualnych baz sygnatur.
	2. Dostęp do najnowszej wersji oprogramowania.
	3. Wsparcia technicznego oprogramowania.
2. Parametry i funkcjonalności dostarczonego oprogramowania, nie mogą być gorsze niż wskazane poniżej:

System musi zapewniać ochronę antywirusową:

a) serwera plików,

b) stacji roboczych,

c) urządzeń przenośnych (smartfony, tablety).

Dla stacji roboczych system musi zapewniać ponadto: ochronę dostępu do sieci (firewall), zapewniać kontrolę podłączanych urządzeń (np. pamięci USB, zewnętrzne napędy, itp.).

Konfiguracja, nadzór nad pracą poszczególnych modułów oraz instalacja musi być wykonywana z centralnej konsoli zarządzającej (Zamawiający posiada już konsolę do zarządzania dla oprogramowania).

Wsparcie techniczne musi odbywać się w języku polskim przez cały czas trwania okres licencji.

Zamawiający wymaga rozwiązania zgłoszonego problemu dotyczącego eksploatacji oprogramowania w ciągu 5 dni roboczych.

Moduł ochrony antywirusowej i antispyware musi poprawnie współpracować
z następującymi systemami operacyjnymi wykorzystywanymi przez Zamawiającego: Microsoft Windows (7 lub wyższą), Microsoft Windows Server (2008 R2 lub wyższą), Linux Ubuntu, CentOS

Moduł ochrony stacji roboczych musi posiadać polskojęzyczny interfejs.

Moduł antywirusowej i antispyware powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hackerskich, oprogramowania typu spyware i adware, rootkit, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.

Moduł ochrony antywirusowej.

Ochrona antywirusowa musi być realizowana na podstawie:

a) sygnatur,

b) heurystyki (z możliwością jej wyłączenia),

c) na bieżąco weryfikowanej informacji o nowych zagrożeniach w bazie producenta dostępnej przez Internet.

Moduł musi mieć możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony.

Moduł musi umożliwiać skanowanie antywirusowe w chwili dostępu (real time), na żądanie i według harmonogramu z następującymi warunkami:

a) skanowanie na żądanie i wg harmonogramu musi mieć możliwość przerwania
w dowolnym momencie,

b) skanowanie na żądanie musi mieć możliwość wstrzymania w przypadku wykrycia pracy na baterii, c) skanowanie na żądanie musi mieć możliwość wstrzymania w przypadku wykrycia pracy w trybie pełnoekranowym (np. prezentacja).

Moduł musi wykrywać zagrożenia: na dyskach, w plikach w tym archiwach plikowych, na stronach web, w przesyłkach email w tym w załącznikach, na podłączanych nośnikach przenośnych.

Moduł musi zapewniać ochronę komunikacji przy wykorzystaniu protokołów POP3, SMTP, IMAP w czasie rzeczywistym niezależnie od klienta pocztowego.

Moduł musi zapewniać ochronę komunikacji przy wykorzystaniu protokołu HTTP
w czasie rzeczywistym niezależnie od przeglądarki.

Moduł musi zawierać warstwę ochronną przeglądarki działającą na stacjach użytkowników i ostrzegające ich o złośliwej zawartości strony internetowej wraz
z możliwością aktywnego blokowania dostępu do wybranych stron internetowych, określonych centralnie przez administratora systemu. Rozwiązanie musi realizować także możliwość określenia blokowanych stron web na podstawie kategorii strony (np. pornografia, strony społecznościowe, itp.).

Moduł musi umożliwiać ustawienia priorytetu procesu skanowania.

Moduł musi umożliwiać aktualizację wzorców wirusów z archiwum internetowego lub z centralnego punktu dystrybucji wzorców wirusów.

Moduł musi umożliwiać pobieranie aktualizacji za pośrednictwem serwera Proxy.

Po wykryciu zagrożenia musi istnieć możliwość oczyszczenia zainfekowanego pliku a jeśli nie jest to możliwe – usunięcia bądź umieszczenia go w lokalnej kwarantannie.

W przypadku zainstalowania na urządzeniach przenośnych musi nastąpić automatyczna zmiana punktu dystrybucji wzorców na archiwum internetowe bez konieczności ingerencji użytkownika.

Moduł musi umożliwiać konfigurowanie dostępności i zakresu ingerencji użytkownika w proces skanowania.

Oprogramowanie musi posiadać centralną konsolę zarządzającą.

Oprogramowanie musi mieć funkcjonalność firewall, umożliwiać ochronę przed atakami z sieci (IDS), ochronę przed botnetami

**[Zasilanie awaryjne]**

**1 szt. zasilacz UPS 5000VA wraz z bateriami oraz usługą montażu**

|  |  |
| --- | --- |
| **Parametr** | **Minimalne wymagane parametry techniczne** |
| **Zastosowanie** | UPS do podtrzymywania napięcia urządzeń serwerowych 230V |
| **Obudowa**  | Nie większa niż 6U, przystosowana do montażu w szafie rack 19” , wraz z wszelkimi akcesoriami wymaganymi do montażu, oraz niezbędnymi do podłączenia z siecią zasilającą |
| **Wyświetlacz** | Wyświetlacz prezentujący podstawowe parametry działania UPS |
| **Wydajność energetyczna** | Conajmniej 5000VA / 5000WCzas podtrzymania przy pełnym obciążeniu 7minSystem przewidywanie stanu akumulatora i daty jego wymiany |
| **Złącza** | * Wyjścia prądowe 8szt w tym minimum 6x C13 (10A), 2x C19 (16A)
* Zarządzanie przez interfejs www, LAN RJ45
* Karta snmp
 |
| **Technologia**  | * Wykonany w technologii On-Line
 |
| **Normy** | * CE, IEC62040-1:2008
 |
| **Gwarancja** | Okres gwarancji 24 miesiące od daty wykonania dostawy. Naprawy gwarancyjne będą realizowane przez producenta urządzenia lub autoryzowanego partnera serwisowego producenta w systemie door-to-door lub u klienta w systemie on-site |