Załącznik Nr 1 do SWZ

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, systemu redundancji danych w chmurze, zarządzalnych urządzeń sieciowych, serwerów fizycznych, serwerowego systemu operacyjnego i oprogramowania bezpieczeństwa, usługi migracji serwerów i systemu ochrony sondą XDR jak Managed Service.

Przeprowadzone zostanie również w ramach zamówienia szkolenie specjalistyczne w zakresie dostarczanych i wdrażanych rozwiązań IT.

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, na repozytorium lokalne bezpieczne od ransomware w postaci dedykowanego urządzenia (appliance), wraz z oprogramowaniem i usługą składającą się z: projekt, wdrożenie, troubleshooting, wsparcie DR w przypadku konieczności odtwarzania środowiska po ataku - 1 szt. Urządzenie do tworzenia kopii bezpieczeństwa 9 TB, 1 szt. Oprogramowanie do tworzenia kopii bezpieczeństwa 7 TB
2. System redundancji danych w chmurze – kopia danych do 5TB w chmurze publicznej.
3. Zarządzalne urządzenia sieciowe – 1 szt. UTM i 1 szt. switch.
4. Serwer fizyczny – 1 szt.
5. Serwerowe systemy operacyjne i oprogramowanie bezpieczeństwa – 2 szt. Serwerowy system operacyjny, 70 szt. licencji dostępowych CAL
6. Migracja serwerów – 1 szt. macierzy dyskowej
7. Ochrona sondą XDR jak Managed Service – 50 szt. licencji oprogramowania antywirusowego.

8. Szkolenia specjalistyczne.

[System zabezpieczenia danych]

Backup środowiska, na repozytorium lokalne bezpieczne od ransomware w postaci dedykowanego urządzenia (appliance), wraz z oprogramowaniem i usługą składającą się z: projekt, wdrożenie, troubleshooting, wsparcie DR w przypadku konieczności odtwarzania środowiska po ataku.

1 szt. Urządzenie do tworzenia kopii bezpieczeństwa 9 TB

1 szt. Oprogramowanie do tworzenia kopii bezpieczeństwa 7 TB

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 dla infrastruktury rozproszonej w kilkunastu lokalizacjach o łącznej pojemności danych backupowanych do 7 TB

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:

1. W ramach realizacji należy dostarczyć projekt, elementy niezbędne do jego realizacji oraz realizację projektu i utrzymanie powstałego systemu według wytycznych ogólnych: Głównym elementem jest centralne, tzn działające w głównej lokalizacji, repozytorium kopii zapasowych. Rolę tą pełni dedykowane, zoptymalizowane i zabezpieczone urządzenie. Składa się ono odpowiednio zaprojektowanego i zabezpieczonego serwera, przestrzeni do zapisywania obrazów backup oraz oprogramowania. Należy je traktować jako zestaw monolityczny uniemożliwiający zastosowanie tego sprzętu w innych celach. Architektura rozwiązania wyróżnia poniższe elementy, ze względu na funkcjonalności jakie realizują:

1.1 Primary serwer – serwer zarządzający i posiadający informacje o pozostałych komponentach środowiska backup,

1.2 Media serwer – serwer przesyłający dane,

1.3 Storage serwer – serwer wykonujący deduplikację inline i przechowujący obrazy backup z opcją WORM

1.4 Klient – system objęty kopią zapasową, wykonujący deduplikację

2. Do poprawnego działania konieczna jest bezpieczna (szyfrowana) komunikacja sieciowa pomiędzy wszystkimi elementami systemu. Aby zoptymalizować wydajność i ograniczyć wymagania dla przepustowości konieczne jest skorzystanie z deduplikacji realizowanej przez klienta.

3. Usługi wsparcia systemu należy dostarczyć przy założeniu sukcesywnego wykorzystania łącznie 24 Roboczodni w systemie zdalnym lub lokalnym realizowane zasobami własnymi oferenta w języku polskim.

Wymagania dla urządzenia

Przez Urządzenie do backupu z deduplikacją danych Zamawiający rozumie rozwiązanie charakteryzujące się jednolitą budową typu „appliance" pochodzące od jednego producenta i realizujące wszystkie wymagane funkcjonalności

Nie dopuszcza się rozwiązania zbudowanego z niezależnych komponentów sprzętowo-programowych

Dostarczone urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych Zamawiającego.

Urządzenie musi spełniać wymagania przedstawione poniżej:

1. Urządzenie musi być przystosowane do montażu w szafie rack 19"

2. Dostarczone urządzenie musi posiadać co najmniej 8 dysków SAS o rozmiarze minimum 2TB (dyski własne urządzenia) oraz 3 dyski NVMe SSD o rozmiarze minimum 1.92TB (dyski własne urządzenia)

3. Oferowane urządzenie musi posiadać przestrzeń na dane po deduplikacji o pojemności minimum 9 TB (powierzchnia czynna) z tym, że musi odbywać się to w obrębie jednego fizycznego urządzenia z półkami dyskowymi

4. Oferowane urządzenie musi umożliwiać rozbudowę przestrzeni na dane po deduplikacji do pojemności minimum 420 TB (powierzchnia czynna) z tym, że musi odbywać się to w obrębie jednego fizycznego urządzenia z półkami dyskowymi. Półki dyskowe muszą być obsadzone minimum 12 dyskami SAS, każdy o rozmiarze maksymalnie 8TB, wraz z kompletem okablowania umożliwiającego podłączenie półek zgodnie z rekomendacjami producenta.

5. Oferowane urządzenie musi posiadać minimum

a. 4 porty Ethernet 1 GbE (wymagane w urządzeniu)

b. 2 porty Ethernet 10/25 GbE z wkładkami SFP+ SR (wymagane w urządzeniu)

c. 2 porty FC 32Gb (wymagane w urządzeniu) dla podłączenia do infrastruktury SAN z dyskami i napędami taśmowymi

6. Oferowane urządzenie musi mieć możliwość (przyszła rozbudowa) dostosowania konfiguracji portów do zmian w infrastrukturze LAN i SAN. Zamawiający musi mieć możliwość zmiany ilości portów urządzenia, tak by po rozbudowie posiadać kombinację:

a. do 4 portów Ethernet 1 GbE (wymagane w urządzeniu)

b. do 6 portów Ethernet 10/25 GbE z wkładkami SFP+ SR (wymagane w urządzeniu)

c. do 8 portów FC 32 Gb w celu rozszerzenia funkcjonalności urządzenia o odbieranie danych od klientów systemu backupowego transmitowanych również przez SAN (wymagane w urządzeniu)

7. Dyski z systemem operacyjnym urządzenia muszą być zabezpieczone technologią nie gorszą niż RAID 1 (lustrzana kopia wolumenu)

8. Przechowywane kopie zapasowe oraz katalog systemu kopii zapasowych muszą być zabezpieczone technologią nie gorszą niż RAID 6 (odporność na awarię w tym samym czasie dwóch dysków)

9. Węzeł obliczeniowy urządzenia musi posiadać minimum 1 dysk hot-spare

10. Każda półka dyskowa urządzenia musi posiadać minimum 1 dysk hot-spare

11. Zarówno węzły obliczeniowe urządzenia jak i półki dyskowe muszą posiadać nadmiarowe zasilacze i wentylatory

12. Zarówno węzły obliczeniowe urządzenia jak i półki dyskowe muszą umożliwiać wymianę dysków, zasilaczy i wentylatorów w trakcie pracy urządzenia (hot-swap)

13. W celu optymalizacji działania i poprawy stanu zabezpieczeń urządzenia, system operacyjny urządzenia oraz zainstalowane na nim oprogramowanie musi być utwardzone (hardened) i zoptymalizowane przez jego producenta

14. Oprogramowanie pokładowe musi umożliwiać śledzenie i zapisywanie w dzienniku zdarzeń wszystkich procesów uruchomionych na urządzeniu

15. Konfiguracja urządzenia musi być możliwa poprzez przeglądarkę internetową i poprzez konsolę znakową

16. Urządzenie musi obsługiwać deduplikację zarówno źródłową, jak i docelową, bez korzystania z serwerów pośredniczących, aby Zamawiający mógł wybrać miejsce deduplikacji w zależności od swoich potrzeb

17. Urządzenia muszą obsługiwać deduplikację zarówno źródłową, jak i docelową, bez korzystania z serwerów pośredniczących, aby Zamawiający mógł wybrać miejsce deduplikacji w zależności od swoich potrzeb. Przy czym muszą umożliwiać wysyłanie zdeduplikowanych i skompresowanych danych do klienta systemu kopii zapasowych bez konieczności rehydracji (proces odwrotny do deduplikacji) i dekompresji przez urządzenie, podnosząc szybkość przywracania danych, zmniejszając ilość przesyłanych danych przez medium transmisyjne i znacznie odciążając zasoby obliczeniowe samego urządzenia

18. W celu uzyskania wysokiej wydajności i odciążenia sieci LAN - urządzenie musi obsługiwać backup i odtworzenia w oparciu o sieć SAN Fiber Channel, w tym bezpośrednie granularne odtworzenie z zdeduplikowanej pamięci masowej. Urządzenia muszą obsługiwać implementację OST over FC

19. Urządzenie musi posiadać zaimplementowane oprócz deduplikacji danych także mechanizmy optymalizujące transfer danych poprzez sieć WAN (tzw: „WAN Optimization”)

20. Urządzenie musi obsługiwać deduplikację na źródle (kliencie), na media serwerze środowiska kopii zapasowych (inline) oraz w urządzeniu (inline)

21. Urządzenie musi oferować wiele poziomów optymalizacji procesu deduplikacji, w tym zmienną długość bloku podczas deduplikacji, automatyczną optymalizację wykorzystania procesora i pamięci, automatyczną optymalizację procesu deduplikacji w zależności od typu backupowanych danych

22. Urządzenie musi wykonywać ciągłą kompleksową weryfikację zdeduplikowanych i przechowywanych kopii zapasowych

23. Urządzenie musi posiadać mechanizm ciągłej weryfikacji cyklicznej kontroli nadmiarowej (CRC) danych kopii zapasowych przechowywanych w puli deduplikacji

24. Urządzenie musi wspierać deduplikację, szyfrowanie i kompresję na źródle oraz w locie podczas zapisu na nośnik dyskowy

25. Urządzenie musi wspierać kompresję i szyfrowanie zdeduplikowanych danych na źródle i zapisanie ich na nośnik dyskowy w niezmienionej postaci

26. Urządzenie musi posiadać funkcjonalność WORM zintegrowaną z oferowanym oprogramowaniem backupu

27. Funkcjonalność WORM musi gwarantować ochronę obrazu kopii zapasowej, tak że jest tylko do odczytu i po utworzeniu kopii zapasowej nie może być modyfikowany, uszkodzony ani zaszyfrowany oraz obraz kopii zapasowej jest chroniony przed usunięciem przed upływem terminu retencji

28. Urządzenie z funkcjonalnością WORM musi umożliwiać obsługę przynajmniej dwóch trybów blokady okresu retencji:

- Nikt nie może nadpisać lub usunąć danych, które są chronione w trybie zgodności w zdefiniowanym okresie retencji. Po ustawieniu okresu przechowywania danych nie można go skrócić, można go jedynie wydłużyć.

- Dedykowany użytkownik może wyłączyć blokadę retencji, a następnie inny użytkownik z odpowiednimi uprawnieniami może usunąć obraz kopii zapasowej.

Wszystkie zdarzenia muszą być rejestrowane w dzienniku urządzenia.

29. Urządzenie musi posiadać wbudowany mechanizm Air Gap odcinający dostęp sieciowy do chronionych danych z wyjątkiem okresu, w którym odbywa się replikacja danych kopii zapasowych.

30. Urządzenie musi wspierać centralne zarządzanie kluczami szyfrowania (KMS) działającym w oferowanym oprogramowaniu backupu

31. Urządzenie musi wspierać szyfrowanie danych z wykorzystaniem minimum protokołu AES

32. Urządzenia muszą posiadać możliwość jednoczesnego dostępu do wewnętrznej deduplikowanej pojemności wszystkimi protokołami czyli: CIFS, NFS, OST, OST dla FC.

33. Wymagane jest dostarczenie urządzenia wraz z licencją, pozwalające na jednoczesną obsługę protokołów CIFS, NFS, OST, OST dla FC do pełnej pojemności urządzenia wraz z dostarczanymi półkami dyskowymi

34. Oferowany produkt musi posiadać obsługę mechanizmów globalnej de-duplikacji dla wszystkich obsługiwanych protokołów, raz otrzymany i zapisany w urządzeniu fragment danych nie może nigdy więcej zostać zapisany bez względu na to, jakim protokołem zostanie ponownie dostarczony

35. Przestrzeń składowania zduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych

36. Oferowane urządzenie musi umożliwiać asynchroniczną replikację/duplikację danych do drugiego urządzenia, konfiguracja replikacji musi być możliwa w każdym z trybów:

- jeden do jednego

- wiele do jednego

- jeden do wielu

37. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu

38. Replikacja/Duplikacja danych między dwoma urządzeniami kontrolowanej przez system backupu musi oferować następujące funkcjonalności:

- replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału dodatkowych serwerów

- replikacji podlegają tylko te fragmenty danych, które nie znajdują się w docelowym urządzeniu

- sterowanie odbywa się z poziomu oferowanego oprogramowania backupu

- oferowane oprogramowanie posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach

39. Urządzenie musi automatycznie usuwać przeterminowane dane (fragmenty danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia

40. Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu)

41. Administracja i konfiguracja urządzeń musi być możliwa poprzez przeglądarkę internetową i poprzez konsolę znakową

41.1 Urządzenia muszą posiadać scentralizowaną konsolę zarządzania, która nie wymaga instalacji dodatkowego oprogramowania w infrastrukturze Zamawiającego.

42. Scentralizowaną konsola zarządzania musi posiadać następujące funkcjonalności:

42.1 Monitorowanie wszystkich zainstalowanych urządzeń w środowisku w jednej konsoli

42.2 Udostępniać informacje o zainstalowanym sprzęcie i oprogramowaniu

42.3 Udostępniać informacje o bieżącej i historycznej (do 30 dni) utylizacji i obciążenia urządzeń

42.4 Porównywać wydajność monitorowanych urządzeń

42.5 Centralnie instalować nowe wersje oprogramowania urządzenia

43. W celu optymalnego planowania pojemności środowiska kopii zapasowych, scentralizowana konsola musi dostarczać następujące informacje o monitorowanych urządzeniach:

43.1 Zajętość wewnętrznej pojemności (%)

43.2 Ilość obsługiwanych zadań systemu kopii zapasowych

43.3 Stopień uzyskanego poziomu deduplikacji (%)

44. W celu monitorowania i planowania wydajności środowiska kopii zapasowych, scentralizowana konsola musi dostarczać informacje o obciążeniu następujących podzespołów monitorowanych urządzeń:

44.1 Procesory (%)

44.2 Pamięć RAM (%)

44.3 Odczyt z dysków urządzenia (MB/s)

44.4 Zapis na dyski urządzenia (MB/s)

44.5 Wydajność sieci (Mb/s)

45. Scentralizowana konsola musi umożliwić eksportowanie informacji minimum w formacie CSV, tak aby była możliwość wykorzystanie informacji w systemach zewnętrznych

46. Urządzenia muszą umożliwiać śledzenie i zapisywanie w dzienniku zdarzeń wszystkich procesów uruchomionych na urządzeniu.

47. Architektura sprzętowa urządzeń musi być zoptymalizowana na potrzeby rozwiązań ochrony danych.

48. System operacyjny urządzeń musi być zoptymalizowany pod kątem zadań ochrony danych i przechowywania danych.

49. System operacyjny urządzeń musi być zoptymalizowany pod kątem bezpieczeństwa i efektywności działania. W szczególności z systemu powinny zostać usunięte wszelkie pakiety zbędne w procesach ochrony danych. W ramach dostarczonej dokumentacji rozwiązania oczekuje się wyspecyfikowania usuniętych pakietów w odniesieniu do standardowej dystrybucji oprogramowania.

50. Producent oferowanych urządzeń musi posiadać lokalną organizację serwisową świadczącą serwis zgodnie z ISO 9001 lub normą równoważną

51. Wszystkie oferowane urządzenia muszą posiadać certyfikat CE (oznakowanie CE - Conformité Européenne) oraz fabryczne oznakowanie

52. Uszkodzone nośniki danych po wymianie pozostają własnością Zamawiającego

53. Serwis gwarancyjny urządzeń musi być realizowany w języku polskim

54. Urządzenie musi mieć możliwość zapisywania dodatkowej zdeduplikowanej kopii danych bezpośrednio do magazynów obiektów publicznej chmury (min. Azure oraz AWS). Zapis danych musi być wykonywany bez wykorzystania serwerów lub urządzeń pośredniczących (zarówno fizycznych jak i wirtualnych). Urządzenie musi mieć możliwość szyfrowania danych przed zapisem do magazynu obiektowego zarządzanym przez Zamawiającego lokalnym kluczem szyfrowania, wymagany algorytm szyfrowania to minimum AES-256 bit. Użytkowane przez Zamawiającego oprogramowanie musi być świadome wykonanej kopii danych i musi mieć możliwość zarządzania czasem retencji poszczególnych kopii danych.

55. Urządzenia muszą posiadać możliwość podziału wewnętrznej pojemności na przestrzeń przeznaczoną na przechowywanie zdeduplikowanych backupów oraz na przestrzeń przeznaczoną na przechowywanie niezdeduplikowanych backupów danych źródłowych, których charakterystyka wyklucza uzyskanie korzyści wynikających z deduplikacji. Mechanizm podziału musi posiadać możliwość elastycznego zarządzania pojemnością przestrzeni zdeduplikowanej i niezdeduplikowanej, tak aby w każdej chwili można było powiększać i zmniejszać każdą z przestrzeni, przekazując pomiędzy nimi zwolnioną pojemność.

Wymagania dla oprogramowania:

1. W celu zapewnienia dużej elastyczności i skalowalności środowiska kopii zapasowych oprogramowanie systemu powinno posiadać trójwarstwową architekturę: Serwer Zarządzający, Serwer Mediów, Klient.

2. Oprogramowanie systemu powinno umożliwiać wykonywanie kopii zapasowych w środowisku heterogenicznym za pomocą, dedykowanego dla platformy systemowej, klienta systemu kopii zapasowych.

3. System powinien umożliwiać łatwą rozbudowę w miarę rozrastania się infrastruktury informatycznej Zamawiającego, poprzez dokładanie kolejnych centralnie zarządzanych Serwerów Mediów.

4 Proponowane rozwiązanie musi umożliwiać uruchomienie serwera zarządzającego kopiami zapasowymi na głównych platformach Windows i Linux.

5. Proponowane rozwiązanie musi wspierać wysoką dostępność (klastrowanie) serwera kontrolującego kopie zapasowe.

6. Oprogramowanie musi być niezależne pod względem sprzętowym i nie może preferować instalacji na platformie sprzętowej jednego producenta. Powinno udostępniać te same funkcjonalności niezależnie od tego na jakiej platformie systemowej będzie zainstalowane. Zamawiający musi posiadać możliwość zmiany platformy sprzętowej bez utraty funkcjonalności systemu kopii zapasowej.

7. Proponowane rozwiązanie musi wspierać wdrożenia na sprzęcie fizycznym, infrastrukturze wirtualnej, w chmurze oraz w kontenerach.

9. Proponowane rozwiązanie musi umożliwiać administrację za pomocą GUI (aplikacja lub web), CLI oraz RESTful API.

9. System powinien posiadać centralną konsolę zarządzania środowiskiem kopii zapasowych. Konsola musi umożliwiać:

9.1 monitorowanie i zarządzanie wszystkimi zadaniami wykonywania i odtwarzania kopii zapasowych, tworzenia duplikatów wykonanych kopii zapasowych,

9.2 ustawianie harmonogramów wykonywania kopii zapasowych,

9.3 monitorowanie i kontrolowanie urządzeń składowania kopii zapasowych podłączonych do Serwerów Mediów,

9.4 centralne zarządzanie konfiguracją, właściwych dla oprogramowania systemu, ustawień Serwera Zarządzającego, Serwera Mediów, Klientów,

9.5 uruchomienie odtwarzania kopii zapasowych na klienta systemu.

10. Oprogramowanie systemu musi posiadać obsługę z poziomu wiersza poleceń w systemach Linux, Unix i Windows. Obsługa z poziomu wiersza poleceń musi umożliwiać:

10.1 konfigurację i modyfikację polityk wykonywania kopii zapasowych,

10.2 konfigurację i modyfikację harmonogramów wykonywania kopii zapasowych,

10.3 konfigurację i modyfikację urządzeń składowania kopii zapasowych podłączonych do Serwerów Mediów,

10.4 konfigurację i modyfikację nośników taśmowych,

10.5 monitorowanie i kontrolowanie zadań kopii zapasowych,

10.6 konfigurację i modyfikację nośników taśmowych

10.7 konfigurację i modyfikację właściwych dla oprogramowania systemu, ustawień Serwera Zarządzającego, Serwera Mediów, Klientów,

10.8 konfigurację, modyfikację i przeglądanie dzienników Serwera Zarządzającego, Serwera Mediów, Klientów.

11. Rozwiązanie powinno być dostępne także jako zintegrowane programowo i sprzętowo urządzenie (appliance), a więc sprzęt i oprogramowanie backupowe razem. Zintegrowane urządzenia powinny umożliwiać zbudowanie w pełni funkcjonującej trzywarstwowej architektury backupowej z funkcjonalnością deduplikacji danych.

12. Baza katalogowa dla systemu backupowego musi być częścią systemu backupowego i wspierać platformy minimum Linux oraz Windows oraz nie powinna posiadać ograniczeń wynikających z ilości używanych w serwerze procesorów i rdzeni procesorów.

13. Baza katalogowa musi być w cenie systemu kopii zapasowych i nie ograniczona co do ilości środowisk backupowych, mocy czy ilości serwerów czy to backupowych czy produkcyjnych. Jakakolwiek rozbudowa środowiska backupowego czy dodanie następnego nie może powodować konieczności dokupienia licencji dla tej bazy.

14. Oprogramowanie systemu kopii zapasowych musi posiadać zintegrowane zarządzanie kluczami szyfrującymi oraz musi posiadać możliwość integracji z zewnętrznymi usługami zarządzania kluczami szyfrowania,

15. Oprogramowanie systemu kopii zapasowych musi integrować się z urządzeniami dyskowymi (deduplikatory) wspierającymi mechanizm WORM w celu ochrony danych przed zaszyfrowaniem, modyfikacją i usunięciem. Funkcjonalność musi zapewniać, że obraz kopii zapasowej jest tylko do odczytu i nie może być modyfikowany, uszkodzony lub zaszyfrowany po utworzeniu kopii zapasowej oraz chronić obraz kopii zapasowej przed usunięciem przed upływem terminu ważności.

16. Obsługa funkcjonalności WORM powinna być realizowana natywnie przez oprogramowanie kopii zapasowych, gdzie zarządzanie czasem ochrony przechowywanych na urządzeniu obrazów kopii zapasowych odbywa się z poziomu oprogramowania systemu backupu, a nie rozdzielnie.

17. Proponowane rozwiązanie musi wspierać ochronę klientów pracujących pod kontrolą:

17.1 Debian 7 - 11,

17.2 Windows 7 - 11,

17.3 Windows Server 2008 - 2022, w tym wydania półroczne,

18. Proponowane rozwiązanie musi wspierać architekturę składowania kopii zapasowych D2D2T i D2D2C.

19. Proponowane rozwiązanie musi obsługiwać dowolny typ pamięci dyskowej (DAS, NAS, SAN) dla repozytorium backupu.

20. Proponowane rozwiązanie musi wspierać storage taśmowy (samodzielne napędy taśmowe oraz biblioteki taśmowe w tym m.in. biblioteki robotów sterowane ACS) głównych producentów.

21. Proponowane rozwiązanie musi deduplikować dane na źródle i celu.

22. Deduplikacja musi umożliwiać wybór pomiędzy zmiennym i stałym rozmiarem bloku. Rozmiar bloku musi umożliwiać jego wybór.

23. Proponowane rozwiązanie musi wspierać deduplikację zarówno inline jak i postprocesową.

24. Proponowane rozwiązanie musi wspierać urządzenia deduplikacyjne głównych producentów takich jak Dell EMC, Exagrid, HPE, Quantum, NEC.

25. Proponowane rozwiązanie musi obsługiwać wirtualne biblioteki taśmowe (VTL).

26. Proponowane rozwiązanie musi wspierać transfer danych zarówno przez sieć LAN jak i SAN.

27. Proponowane rozwiązanie musi wspierać głównych dostawców chmur publicznych jako magazyn kopii zapasowych.

28. Proponowane rozwiązanie musi obsługiwać deduplikację do chmury w celu minimalizacji transferu danych.

29. Proponowane rozwiązanie musi umożliwiać wznowienie nieudanego zadania backupowego od ostatniego punktu kontrolnego.

30. Proponowane rozwiązanie musi automatyzować tworzenie wielu kopii zapasowych na różnych urządzeniach magazynowych z różną długością przechowywania danych.

31. Proponowane rozwiązanie powinno posiadać możliwość wykonywania wysokowydajnych kopii zapasowych serwerów z bardzo obciążonymi systemami plików na dyskach z dużą liczbą plików (np. backup typu disk-image).

32. Proponowane rozwiązanie musi zapewniać możliwość wykonywania backupu syntetycznego.

33. Proponowane rozwiązanie musi umożliwiać tworzenie ręcznych kopii zapasowych ad-hoc.

34. Proponowane rozwiązanie musi wspierać topologie replikacji danych typu jeden-do-jednego, wiele-do-jednego, jeden-do-wielu oraz kaskadową z wykorzystaniem deduplikacji danych w celu zminimalizowania ilości przesyłanych danych.

35. Proponowane rozwiązanie musi wspierać szyfrowanie danych.

36. Proponowane rozwiązanie musi umożliwiać wznowienie nieudanego zadania przywracania z ostatniego punktu kontrolnego

37. Proponowane rozwiązanie musi zapewniać funkcje umożliwiające natywne odzyskiwanie "bare metal" (w pełni zautomatyzowane odzyskiwanie obejmujące system operacyjny, konfigurację, aplikacje i dane) klientów Windows, Linux bez konieczności korzystania z zewnętrznych/rodzimych narzędzi do odzyskiwania/reimaging systemu operacyjnego.

38. Proponowane rozwiązanie musi umożliwiać przywracanie różnych konfiguracji systemu oraz różnych układów dysków.

39. Proponowane rozwiązanie musi zapewniać możliwość konwersji P2V i V2P.

40. Proponowane rozwiązanie musi umożliwiać przywracanie nawet po wygaśnięciu wsparcia technicznego oprogramowania.

41. Proponowane rozwiązanie musi umożliwiać przywracanie pojedynczych obiektów Active Directory z kopii zapasowej Windows System State.

Backup

1. Proponowane rozwiązanie musi wspierać VMware vSphere 6.0 i nowsze.

2. Proponowane rozwiązanie musi wspierać serwery vSphere zarządzane przez vCenter jak i samodzielne serwery ESXi.

3. Proponowane rozwiązanie musi wspierać VMware vSAN 6.5 i nowsze.

4. Proponowane rozwiązanie musi wspierać VMware vCloud Director 9.x.

5. Proponowane rozwiązanie musi wspierać wszystkie tryby transportu danych obsługiwane przez VDDK 6.7.2 (SAN, NBD, NBDSSL, hot-add).

6. Proponowane rozwiązanie nie może wymagać instalacji agentów w maszynach wirtualnych w celu wykonywania kopii zapasowych.

7. Proponowane rozwiązanie musi wspierać śledzenie zmian (CBT - change block tracking).

8. Proponowane rozwiązanie musi wspierać tworzenie syntetycznych kopii zapasowych (tworzonych na podstawie ostatniego pełnego backupu oraz backupu przyrostowego CBT) maszyn wirtualnych VMware w celu umożliwienia wykonywania backupów przyrostowych (incremental-forever).

9. Proponowane rozwiązanie musi zawierać mechanizm automatycznego wykrywania i ochrony maszyn wirtualnych VMware bez konieczności zmiany polityk backupu.

10. Proponowane rozwiązanie musi umożliwiać wyłączenie z backupu maszyn wirtualnych VMware usuniętych bloków oraz pliku swap.

11. Proponowane rozwiązanie musi wspierać przywracanie pojedynczego pliku z kopii zapasowej maszyny wirtualnej VMware bez konieczności uruchamiania agenta w maszynie wirtualnej oraz umieszczania wirtualnego dysku w tymczasowej lokalizacji, jeżeli obraz kopii zapasowej jest przechowywany na taśmach.

12. Proponowane rozwiązanie musi wspierać jednoprzebiegowy backup Microsoft SQL Server z możliwością przywracania elementów granularnych zgodnie z opisem w dalszej części.

13. Proponowane rozwiązanie nie może wymagać wykonywania osobnego backupu na poziomie aplikacji backupu na poziomie aplikacji lub wysyłki logów w przypadku backupu Microsoft SQL Server.

14. Proponowane rozwiązanie musi wspierać limitowanie zasobów takich jak liczba jednoczesnych zadań backupu na serwer ESXi, klaster lub magazyn danych.

15. Proponowane rozwiązanie musi umożliwiać uruchomienie maszyny wirtualnej bezpośrednio z dyskowego repozytorium kopii zapasowych.

16. Proponowane rozwiązanie musi zapewniać natychmiastowy dostęp do chronionych maszyn wirtualnych i ich plików.

17. Proponowane rozwiązanie musi zapewniać dodatkowe możliwości administracji, monitorowania i odzyskiwania danych poprzez VMware vCenter Web Client.

Backup oprogramowania do wirtualizacji fizycznych maszyn

1. Proponowane rozwiązanie musi wspierać Microsoft Hyper-V 2008 SP2 i nowsze.

2. Proponowane rozwiązanie musi wykorzystywać Windows Management Instrumentation (WMI) dla ochrony maszyn wirtualnych działających na platformie Hyper-V 2016 i nowszych.

3. Proponowane rozwiązanie musi wspierać ochronę maszyn wirtualnych rezydujących na systemach plików NTFS, ReFS, Windows Storage Spaces, Storage Spaces Direct oraz SMB 3.0.

4. Proponowane rozwiązanie musi wspierać Resilient Change Tracking (RCT).

5. Proponowane rozwiązanie musi wspierać tworzenie syntetycznych kopii zapasowych (tworzonych na podstawie ostatniego pełnego i przyrostowego backupu RCT) maszyn wirtualnych Hyper-V w celu umożliwienie tworzenia kopii zapasowych przyrostowych na zawsze.

6. Proponowane rozwiązanie musi wspierać ograniczenie liczby aktywnych snapshotów lub backupów na serwer Hyper-V i klaster.

7. Proponowane rozwiązanie musi zawierać mechanizm automatycznego wykrywania i ochrony maszyn wirtualnych Hyper-V VM bez konieczności zmiany polityk backupu.

8. Proponowane rozwiązanie musi umożliwiać wykluczenie usuniętych bloków i plików swap z kopii zapasowej maszyny wirtualnej Hyper-V.

9. Proponowane rozwiązanie musi wspierać wyłączenie dysków startowych z backupu maszyn wirtualnych Hyper-V z kopii zapasowych maszyn wirtualnych Hyper-V

10. Proponowane rozwiązanie musi wspierać wyłączenie dysków danych z backupu maszyn wirtualnych Hyper-V kopii zapasowej maszyny wirtualnej

11. Proponowane rozwiązanie musi wspierać przywracanie pojedynczego pliku z kopii zapasowej maszyny wirtualnej Hyper-V bez konieczności przenoszenie dysku wirtualnego w lokalizacji tymczasowej, jeżeli obraz kopii zapasowej jest przechowywany na taśmach

12. Proponowane rozwiązanie musi zapewniać integrację z System Center Virtual Machine Manager (SCVMM) w celu umożliwienia odzyskiwania maszyn wirtualnych

Backup MS SQL Server

1. Proponowane rozwiązanie musi wspierać Microsoft SQL Server 2016 i nowsze.

2. Proponowane rozwiązanie musi wspierać SQL Server Availability Groups.

3. Proponowane rozwiązanie musi wspierać automatyczne wykrywanie instancji SQL.

4. Proponowane rozwiązanie nie powinno wymagać skryptów wsadowych tworzonych przez użytkownika, które posiadały instrukcje tworzenia kopii zapasowych instancji baz danych SQL oraz logów transakcyjnych.

5. Proponowane rozwiązanie musi zapewniać wykonywanie pełnych, różnicowych i dzienników transakcji kopii zapasowych baz danych SQL.

6. Proponowane rozwiązanie nie może wykorzystywać metody log-shipping do ochrony logów transakcyjnych SQL.

7. Proponowane rozwiązanie musi umożliwiać wykonywanie kopii zapasowych MS SQL Server poza hostem SQL Server, Instant Recovery oraz wykonywanie kopii zapasowych u dostawcy sprzętu.

8. Proponowane rozwiązanie musi wspierać pełne przywracanie i odzyskiwanie baz danych SQL.

9. Proponowane rozwiązanie musi wspierać przywracanie grup plików SQL.

10. Proponowane rozwiązanie musi wspierać przywracanie plików bazy danych SQL.

11. Proponowane rozwiązanie musi wspierać przywracanie logów transakcyjnych SQL do określonego punktu w czasie.

12. Proponowane rozwiązanie musi wspierać przywracanie logu transakcyjnego SQL do określonego punktu w czasie konkretnej transakcji.

Backup NDMP

1. Proponowane rozwiązanie musi wspierać wykorzystanie protokołu Network Data NDMP (Network Data Management Protocol) do inicjowania i sterowania kopiami zapasowymi i przywracaniem systemów NAS (Network Attached Storage).

2. Proponowane rozwiązanie musi obsługiwać NDMP v2, v3 i v4.

3. Proponowane rozwiązanie musi wykorzystywać techniki wykrywania zmian w filerze w celu identyfikacji modyfikacji, które nastąpiły od momentu wykonania ostatniego backupu.

4. Proponowane rozwiązanie musi obsługiwać lokalne i trójstronne kopie zapasowe NDMP.

5. Proponowane rozwiązanie musi obsługiwać funkcję NDMP DirectCopy.

6. Proponowane rozwiązanie musi umożliwiać przywracanie pojedynczych plików z kopii zapasowych NDMP.

7. Proponowane rozwiązanie musi obsługiwać funkcję NDMP Direct Access Recovery (DAR).

Snapshots

1. Proponowane rozwiązanie musi zapewniać możliwość wykonywania migawek minimum dla następujących macierzy dyskowych:

1.1. Pure Storage FlashArray

1.2 macierze pamięci masowej HPE 3PAR

1.3 macierze pamięci masowej NetApp

1.4 Hitachi storage array

1.5 macierze klasy enterprise InfiniBox

2. Możliwość wykonywania migawek musi być dostępna dla systemów operacyjnych Windows i Linux

Raportowanie

1. Proponowane rozwiązanie musi zapewniać podstawowe i zaawansowane raportowanie, w tym m.in. ale nie tylko; raportowanie kosztów zwrotnych, oszczędności deduplikacji, statystyki backupu, raportów

o błędach, raportów na poziomie biznesowym do celów prognozowania, raportowanie SLA w zakresie backupu i odzyskiwania danych.

2. System raportowania rozwiązania powinien umożliwiać automatyczne wysyłanie wiadomości e-mail automatycznie codziennie jako załączniki w formacie .pdf, .csv i html.

3. Proponowane rozwiązanie musi posiadać możliwość centralnego zarządzania, monitorowania i raportowania w odniesieniu do środowisk oprogramowania i urządzeń, w tym wielu środowisk backupowych.

4. Proponowane rozwiązanie musi umożliwiać wysyłanie powiadomień o zadaniach za pomocą poczty elektronicznej lub SNMP.

Odporność na Ransomware

1. Proponowane rozwiązanie musi posiadać wbudowany mechanizm wykrywania i powiadamiania o podejrzanych zmianach podczas tworzenia kopii zapasowych.

2. Proponowane rozwiązanie musi posiadać własny skaner złośliwego oprogramowania oraz mieć możliwość integracji z zewnętrznymi skanerami złośliwego oprogramowania w celu skanowania składowanych obrazów kopii zapasowych.

3. Proponowane rozwiązanie musi posiadać możliwość automatycznego wstrzymywania zadań kopii zapasowych dla chronionego zasobu po wykryciu infekcji w jego kopii zapasowej, powinno obejmować tworzenie nowych kopii zapasowych, ich powielanie i wygaszanie.

4. Proponowane rozwiązanie musi posiadać możliwość identyfikowania ostatniej znanej dobrej kopii zapasowej przed przywróceniem maszyny wirtualnej.

5. Proponowane rozwiązanie musi posiadać możliwość integracji z platformami SOAR/XDR w celu wstrzymywania lub wznowienia zadań związanych z ochroną danych na podstawie zdarzeń związanych z bezpieczeństwem lub pracami serwisowymi. Powiadomienia o anomaliach i skanowaniu złośliwego oprogramowania przechowywane w dziennikach oprogramowania muszą być łatwo pobierane przez systemy wczesnego ostrzegania, takie jak platformy SIEM.

Multi-tenancy

1. Proponowane rozwiązanie musi umożliwiać tworzenie logicznie odizolowanych środowisk dla różnych organizacji/działów (Multi-Tenancy).

2. Proponowane rozwiązanie musi wspierać kontrolę dostępu opartą na rolach (RBAC).

3. Proponowane rozwiązanie musi oferować samoobsługowy backup i przywracanie danych dla wielu użytkowników, w sposób bezpieczny i podzielony na partycje.

Disaster Recovery Readiness

1. Proponowane rozwiązanie powinno zapewniać pojedynczy pulpit nawigacyjny do śledzenia stanu gotowości do Disaster Recovery wszystkich wybranych aplikacji.

2. Proponowane rozwiązanie musi zapewniać pełną automatyzację wszystkich operacji związanych z niezawodnością przy udziale maszyn wirtualnych, aplikacji i wielowarstwowych usług biznesowych.

3. Proponowane rozwiązanie powinno być w stanie zaoferować prawdziwe Disaster Recovery, jak również możliwości migracji, aby być w stanie zrealizować różne aspekty planu ciągłości biznesowej,

takie jak odzyskiwanie do istniejącej i/lub zdalnej lokalizacji, migracja/odzysk do wybranej chmury publicznej.

4. Proponowane rozwiązanie powinno umożliwiać definiowanie aplikacji wielowarstwowych, tak aby wszystkie warstwy aplikacji były migrowane do miejsca Disaster Recovery lub testowane jako jedna całość.

5. Proponowane rozwiązanie powinno być w stanie zapewnić spójne wsparcie dla platform fizycznych i wirtualnych, w tym cross-hypervisor (konwersja maszyn wirtualnych) oraz oferować opcję odzyskiwania do technologii chmurowych.

6. Proponowane rozwiązanie powinno być w stanie zapewnić wielostanowiskową widoczność stanu zdrowia komponentów aplikacji w czasie rzeczywistym.

7. Proponowane rozwiązanie powinno wspierać wiele celów poziomu usług (Service Level Objectives) w tym RPO backupu/odtwarzania.

8. Rozwiązanie powinno umożliwiać automatyczne wykonywanie procesów Disaster Recovery i odzyskiwania w trybie symulacji, bez żadnych trwałych zmian w środowisku Disaster Recovery, aby potwierdzić czy wszystkie wymagania są spełnione dla pomyślnego wykonania procedury Disaster Recovery. Powinno ono wspierać testy nienaruszające produkcyjną infrastrukturę.

9. Rozwiązanie DR powinno posiadać mechanizm zarządzania uprawnieniami oparte o role i powinno wykorzystywać istniejące Active Directory/LDAP do zarządzania tożsamością.

10. Proponowane rozwiązanie musi posiadać własny mechanizm do replikacji danych, a także umożliwiać wykorzystanie mechanizmów innych producentów w celu zwiększenia elastyczności.

11. Proponowane rozwiązanie replikacji musi obsługiwać zarówno platformy fizyczne jak i wirtualne z wbudowaną kompresją.

12. Proponowane rozwiązanie powinno umożliwiać planowanie działań lub testów w przyszłych terminach, a rozwiązanie powinno automatycznie, bez żadnych zależności, inicjować procesy zaplanowanych terminach. Alerty również powinny być generowane i powiadamiać administratora z wyprzedzeniem.

13. Proponowane rozwiązanie powinno mieć możliwość zatrzymania/pauzy/wznowienia w trakcie wykonywania skonfigurowanego wcześniej procesu.

14. Proponowane rozwiązanie powinno udostępniać status uruchomionego procesu w trakcie jego wykonywania.

15. Proponowane rozwiązanie musi zapewniać dowód zgodności z wewnętrznymi i zewnętrznymi wymogami ciągłości biznesowej za pomocą raportów z audytów i nieprzerwanych testów odzyskiwania danych po awarii w czasie rzeczywistym.

16. Proponowane rozwiązanie musi zapewniać pełną automatyzację wszystkich operacji związanych z odpornością, w tym rejestrów uruchomień odzyskiwania oraz orkiestracji uruchamiania i zatrzymywania odzyskiwania dla aplikacji wielowarstwowych w celu zmniejszenia ryzyka przestojów spowodowanych błędami ludzkimi.

[System redundancji danych w chmurze]

Kopia danych do 5 TB w chmurze publicznej

Przedmiotem zamówienia jest rozwiązanie kopii danych do 5 TB w chmurze publicznej jako zabezpieczenie DR na okoliczność incydentów cybernetycznych i fizycznych, lokalizacja danych - Polska. Usługa na okres 2 lat.

1. Usługa musi oferować wysoce dostępny, wysoce skalowalny, trwały i bezpieczny magazyn dla różnych obiektów danych w chmurze publicznej.

2. Obiekty danych muszą być dostępne z dowolnego miejsca na świecie za pośrednictwem protokołu HTTP lub HTTPS oraz za pośrednictwem interfejsu API REST.

3. Usługa powinna również oferować biblioteki klienckie dla deweloperów tworzących aplikacje lub usługi za pomocą platformy .NET, Java, Python, JavaScript, C++i Go.

4. Deweloperzy i specjaliści IT muszą mieć możliwość używania komend i skryptów programu PowerShell.

5. Dostęp do zarządzania usługą powinna być z poziomu witryny internetowej i dedykowanego oprogramowania.

6. Przedmiot zamówienia powinien odznaczać się następującymi cechami:

6.1 niezawodność i wysoka dostępność uzyskana dzięki kopiom i replikom. Tak uzyskana nadmiarowość powinna zapewnić bezpieczeństwo danych w przypadku przejściowych awarii sprzętu. Replikacja powinna być dostępna na poziomie centrów przetwarzania danych i/lub regionów geograficznych.

6.2 posiada mechanizm szyfrowania danych w celu zapewnienia bezpieczeństwa

6.3 usługa musi być zaprojektowana jako wysoce skalowalne rozwiązanie spełniające potrzeby związane z magazynowaniem danych i wydajnością współczesnych aplikacji.

6.4 dostępność na poziomie globalnym. Dane muszą być dostępne z dowolnego miejsca na świecie za pośrednictwem protokołu HTTP lub HTTPS. Biblioteki klienckie muszą być dostępne w różnych językach, w tym .NET, Java, Node.js, Python, Go i innych. Usługa musi być także kompatybilna z interfejsem API REST. Usługa musi obsługiwać skrypty programu PowerShell lub interfejsu wiersza poleceń. Praca z danymi powinna się odbywać albo za pośrednictwem dedykowanej witryny internetowej, albo dedykowanego oprogramowania.

7. Przedmiot zamówienia musi zawierać następujące usługi:

7.1 wysoce skalowalny magazyn obiektów dla danych tekstowych i binarnych do obsługi i analizy danych big data

7.2 zarządzane udziały plików dla wdrożeń lokalnych lub w chmurze.

7.3 magazyn obsługi komunikatów zapewniający niezawodną obsługę komunikatów między składnikami aplikacji.

7.4 magazyn obiektów NoSQL do magazynowania ustrukturyzowanych danych bez użycia schematu.

7.5 usługi zarządzania woluminami, wdrażania i aranżacji utworzone natywnie dla kontenerów.

7.6 każda z wymienionych usług musi być dostępna za pośrednictwem konta magazynu z unikatowym adresem.

8. Dostawca usługi musi gwarantować możliwość wyboru lokalizacji przechowywania danych przynajmniej w 5 lokalizacjach w Europie.

[Zarządzalne urządzenie sieciowe]

A. 1 szt. UTM

Minimalne wymagania dla jednej sztuki urządzenia UTM

1. Wymagania Ogólne

1.1 System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

1.2 System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

1.3 System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

1.4 System wspiera protokoły IPv4 oraz IPv6 w zakresie:

1.4.1 Firewall.

1.4.2 Ochrony w warstwie aplikacji.

1.4.3 Protokołów routingu dynamicznego.

2. Redundancja, monitoring i wykrywanie awarii

2.1 W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.

2.2 Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

2.3 Monitoring stanu realizowanych połączeń VPN.

2.4 System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

3. Interfejsy, Dysk, Zasilanie:

3.1 System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

3.1.1 5 portami Gigabit Ethernet RJ-45.

3.2 System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3.3 System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.

3.4 System jest wyposażony w zasilanie AC.

4. Parametry wydajnościowe:

4.1 W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.

4.2 Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.

4.3 Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.

4.4 Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.

4.5 Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.

4.6 Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.

4.7 Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

5. Funkcje Systemu Bezpieczeństwa:

5.1 W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

5.1.1 Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

5.1.2 Kontrola Aplikacji.

5.1.3 Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

5.1.4 Ochrona przed malware.

5.1.5 Ochrona przed atakami - Intrusion Prevention System.

5.1.6 Kontrola stron WWW.

5.1.7 Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

5.1.8 Zarządzanie pasmem (QoS, Traffic shaping).

5.1.9 Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

5.1.10 Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.

5.1.11 Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

5.1.12 Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

6. Polityki, Firewall

6.1 Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

6.2 System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

6.2.1 Translację jeden do jeden oraz jeden do wielu.

6.2.2 Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

6.3 W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

6.4 Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.

6.5 Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

6.6 Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

6.7 Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

6.7.1 Amazon Web Services (AWS).

6.7.2 Microsoft Azure.

6.7.3 Cisco ACI.

6.7.4 Google Cloud Platform (GCP).

6.7.5 OpenStack.

6.7.6 VMware NSX.

6.7.7 Kubernetes.

7. Połączenia VPN

7.1 System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

7.1.1 Wsparcie dla IKE v1 oraz v2.

7.1.2 Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).

7.1.3 Obsługa protokołu Diffie-Hellman grup 19, 20.

7.1.4 Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.

7.1.5 Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

7.1.6 Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.

7.1.7Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

7.1.8 Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.

7.1.9 Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.

7.1.10 Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.

7.1.11 Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.

7.1.12 Mechanizm „Split tunneling” dla połączeń Client-to-Site.

7.2 System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

7.2.1 Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

7.2.2 Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

8. Routing i obsługa łączy WAN. W zakresie routingu rozwiązanie zapewnia obsługę:

8.1 Routingu statycznego.

8.2 Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).

8.3 Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.

8.4 Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.

8.5 ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.

8.6 BFD (Bidirectional Forwarding Detection).

8.7 Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

9. Funkcje SD-WAN

9.1 System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

9.2 SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

10. Zarządzanie pasmem

10.1 System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

10.2 System daje możliwość określania pasma dla poszczególnych aplikacji.

10.3 System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.

10.4 System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

11. Ochrona przed malware

11.1 Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

11.2 Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.

11.3 System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.

11.4 System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.

11.5 System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

11.6 Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

11.7 System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.

11.8 Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

11.9 Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

12. Ochrona przed atakami

12.1 Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

12.2 System chroni przed atakami na aplikacje pracujące na niestandardowych portach.

12.3 Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

12.4 Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.

12.5 System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

12.6 Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).

12.7 Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

12.8 Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

13. Kontrola aplikacji

13.1 Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

13.2 Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

13.3 Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

13.4 Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

13.5 Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.

13.6 Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).

13.7 System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

14. Kontrola WWW

14.1 Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

14.2 W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

14.3 Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.

14.4 Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

14.5 Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).

14.6 Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.

14.7 Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.

14.8 Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.

14.9 System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

15. Uwierzytelnianie użytkowników w ramach sesji

15.1 System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:

15.1.1 Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

15.1.2 Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

15.1.3 Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

15.2 System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.

15.3 System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.

15.4 Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

16. Zarządzanie

16.1 Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.

16.2 Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.

16.3 Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

16.4 System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.

16.5 System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

16.6 Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

16.7 Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

16.8 Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).

16.9 Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

17. Logowanie

17.1 Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

17.2 W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

17.3 Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.

17.4 Możliwość włączenia logowania per reguła w polityce firewall.

17.5 System zapewnia możliwość logowania do serwera SYSLOG.

17.6 Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

18. Certyfikaty – poszczególne elementy systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

18.1 EAL4 dla funkcji Firewall.

19. Testy wydajnościowe oraz funkcjonalne

19.1 Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

20. Serwisy i licencje Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

20.1 Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [x] miesięcy.

21. Gwarancja oraz wsparcie

21.1 Gwarancja: System jest objęty serwisem gwarancyjnym, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu wykonawca zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

B. 1 szt. switch

1. Parametry fizyczne platformy:

1.1 wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U

1.2 Zasilanie 230V

1. MTBF > 10lat

2. Interfejsy sieciowe – wymagania minimalne:

2.1 24 porty GE, RJ-45

2.2 4 porty 10GE SFP+

2.3 24 portów umożliwiających zasilanie PoE 802.3af/at o sumarycznym budżecie mocy 370W – dla wersji z FPOE

3. Zarządzanie:

3.1 port konsoli szeregowej RJ45

3.2 Zarządzanie przez wiersz poleceń (SSH) oraz poprzez graficzny interfejs poprzez przeglądarkę

4. Parametry wydajnościowe:

4.1 przepustowość urządzenia - min. 128 Gbps, min. 190 Mpps

4.2 możliwość zapamiętania co najmniej 32 000 adresów MAC

4.3 Opóźnienie - poniżej 1 mikrosekundy

4.4 Bufor pakietów: min. 2 MB

4.5 Pamięć DRAM: min. 512 MB

4.6 Pamięć FLASH: min. 64 MB

5. Wymagane funkcje:

5.1 możliwość automatycznej negocjacji prędkości i duplexu dla połączeń

5.2obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree)

5.3 możliwość agregacji portów zgodna z 802.3ad

5.4 obsługa co najmniej 4000 VLANów, zgodna z 802.1Q

5.5 możliwość wykonywania routingu statycznego (realizowany software'owo)

5.6 port-mirroring

5.7 Kontrola dostępu na poziomie portu w oparciu o standard 802.1x, możliwość uwierzytelniania w oparciu o bazę Radius

5.8 zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS, SNMP w wersjach 1-3, SNTP, LLDP (w trybie odbioru)

5.8 możliwość zarządzania przez interfejs graficzny i tekstowy

5.10 możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI

5.11 możliwość integracji z systemem bezpieczeństwa NGFW, w zakresie co najmniej:

5.11.1 możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników

5.11.2 obsługa białych i czarnych list MAC

5.11.3 stateful firewall, umożliwiający kontrolę dostępu do sieci

5.11.4 routing statyczny i dynamiczny, co najmniej OSPF

6. Moduły sieciowe:

6.1 Wraz z przełącznikami należy dostarczyć następujące moduły sieciowe:

6.2 Moduły 10GE SFP+ transceiver module – 4 szt.

6.3 Moduły muszą być oficjalnie wspierane przez producenta urządzeń.

7. Gwarancja oraz wsparcie:

7.1 Dożywotnia Gwarancja: urządzenia muszą być objęte dożywotnią gwarancją, gwarantującą wymianę wadliwego sprzętu (okres 5 lat od ogłoszenia zakończenia produkcji).

7.2 Wsparcie serwisowe: System powinien być objęty serwisem gwarancyjnym przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.

[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. Ramka musi umożliwiać włączenie i wyłączenie podświetlenia umożliwiając lepszą identyfikację serwera.

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

3.2 Obsługa minimum 4 TB RAM. Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci RAM DDR5.

4. Procesor

4.1 Dwa procesory wielordzeniowe osiągające w teście PassMark CPU Mark wynik min. 49.000 pkt według danych ze strony https://www.cpubenchmark.net/multi_cpu.html dla konfiguracji wieloprocesorowej

5. Pamięć RAM

5.1 Zainstalowana pamięć RAM minimum 128 GB RDIMM DDR5 lub LRDIMM.

5.2 Rozmiar pojedynczej kości pamięci RAM 32GB

5.3 Możliwość rozbudowy do minimum 1,5 TB.

5.4 Memory mirroring, ECC, patrol scrubbing, SDDC, memory thermal throttling, ADDDC-SR, PPR, Memory SMBus hang recovery.

6. Pamięć masowa

6.1 Minimum 8 dysków 1.92TB 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.

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 TYP-C na przednim panelu obudowy, musi umożliwiać dostęp do modułu zarządzania serwerem poprzez bezpośrednie połączenie.

9.3 Minimum 1 port VGA.

10. Interfejsy sieciowe

10.1 Sumarycznie minimum cztery interfejsy sieciowe 10 GbE BASE-T zapewnione przez minimum 2 karty sieciowe (Po 2 interfejsy 10 GbE 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 o mocy minimum 1600W 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.

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 myszy i klawiatury, montowanie wirtualnych napędów, zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego, wysyłanie zawiadomień droga mailową i poprzez SNMP. Wsparcia dla IPMI, SSH, Redfish. Wparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows. Nadawanie ról użytkownikom. Możliwość zarządzania minimum 200 serwerami z poziomu modułu zarządzającego pojedynczego serwera, na tym etapie dodatkowe licencje nie są wymagane. Możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem. Serwer umożliwia wykonanie aktualizacji oprogramowania do zarządzania serwerem, BIOS.

14.3 Możliwość zarządzania zdalnego poprzez darmową aplikację mobilną producenta serwera dostępną w AppStore dla systemów iOS. Aplikacja musi umożliwiać podłączenie do serwera przez sieć wi-fi lub przez port USB na froncie obudowy. Aplikacja musi umożliwiać:

14.3.1 sprawdzenie aktualnego poboru mocy przez zasilacze

14.3.2 sprawdzenie temperatury powietrza na wlocie do serwera

14.3.3 sprawdzenie modelu kontrolera RAID oraz utworzonych dysków fizycznych i logicznych

14.3.4 sprawdzenie ilości zainstalowanych modułów pamięci, pojemności, taktowania, numerów seryjnych i slotu w którym są zainstalowane

14.3.5 sprawdzenie zainstalowanych procesorów, taktowania zegara ilości rdzeni, wątków oraz pamięci Cache

14.3.6 wyświetlanie alarmów dot. pracy serwera z podziałem na kategorie według istotności

14.3.7 konfiguracje adresacji IP portu management port

14.3.8 włączenie oraz wyłączenie serwera

14.3.9 sprawdzenie wersji firmware

15. Certyfikaty i Deklaracje

15.1 Deklaracja zgodności UE (Certyfikat CE).

15.2 Certyfikat zgodności z dyrektywą RoHS lub dokument wystawiony przez niezależną, akredytowaną jednostkę potwierdzający spełnienie kryteriów środowiskowych zgodnych z dyrektywą RoHS o eliminacji substancji niebezpiecznych.

15.3 Serwer musi być zaprojektowany i produkowany zgodnie z normą ISO-9001 lub równoważną oraz zaprojektowany i produkowany zgodnie z normą ISO-14001 lub równoważną.

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 w trybie 9x5 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 Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:

16.4.1 możliwość pobierania najnowszego firmware.

16.4.2 dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń.

16.4.3 otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware.

[Serwerowe systemy operacyjne i oprogramowanie bezpieczeństwa]

2 szt. Serwerowy system operacyjny.

Zamawiający aktualnie korzysta z oprogramowania typu Microsoft Windows Server 2022 Standard i wymagana dostarczenia licencji na oprogramowanie Microsoft Windows Server 2022 Standard 16-core lub nowszy.

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.

70 szt. licencji dostępowych Windows Server 2022 User CAL lub równoważne

Minimalne wymagania dotyczące licencji dostępowej typu User CAL do oprogramowania Microsoft Windows Server 2022 Standard Edition 16-core lub nowszej.

1. Przedmiotem zamówienia jest 70 szt. licencji dostępowej typu User CAL do oprogramowania Microsoft Windows Server 2022 Standard Edition 16-core.

2. Jedna licencja dostępowa musi umożliwić jednemu użytkownikowi dostęp do systemu z dowolnego urządzenia pozostającego w tej samej domenie, co Windows Server.

3. Posiadacz licencji na użytkownika musi mieć możliwość korzystania z funkcji systemu Windows Server z różnych urządzeń m.in. stacjonarnych i mobilnych.

W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do zaoferowania odpowiednich licencji dostępowych do zaproponowanego

oprogramowania oraz pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania.

[Migracja serwerów]

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 10 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 Budowa systemu musi umożliwiać rozbudowę do modeli wyższych bez potrzeby kopiowania/migrowania danych (zamawiający przez model wyższy rozumie inny model macierzy danego producenta z większą pamięcią cache oraz mocniejszymi procesorami).

2.5 Zamawiający dopuszcza rozwiązanie, które nie pozwala na rozbudowę do wyższego modelu przy założeniu, że zostanie zaoferowany najwyższy model z rodziny z pamięcią Cache min 1TB na kontroler.

2.6 System musi mieć możliwość rozbudowy do 500 dysków w obrębie pary kontrolerów lub w obrębie klastra wielu kontrolerów (scale-out) w zależności od sposobu realizacji rozbudowy dla oferowanego rozwiązania.

2.7 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.

2.8 Dla rozwiązań wykorzystujących klastrowanie (scale-out) musi być możliwość rozbudowy rozwiązania do co najmniej 12 kontrolerów w klastrze.

2.9 Rozwiązanie musi pozwalać na rozbudowę o dyski lub kontrolery wykonane w technologii NVMe do min 1120 dysków w technologii NVME. Zamawiający dopuszcza zaoferowanie rozwiązania, które nie posiada takiej możliwości w przypadku, gdy całość zasobów zostanie dostarczona na dyskach flash/SSD.

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 do 6TB.

4. Interfejsy

4.1 Oferowana macierz musi posiadać minimum

4.1.1 4 porty 10GbE SFP+

4.1.2 4 porty 16Gb FC bez wkładek SFP

4.1.3 2 porty 1Gb do zarządzania

4.1.4 4 porty 12Gb SAS

4.2 Macierz musi pozwalać na zamianę wkładek z 10GbE na 16Gb FC.

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, Unix

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. Macierz powinna mieć możliwość czynności odwrotnej tzn. Cofnięcia procesu deduplikacji na zdeduplikowanym wolumenie. 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. Przed procesem replikacji macierz musi umożliwiać włączenie procesu deduplikacji danych w celu optymalizacji wykorzystania łącza dla replikowanych zasobów lub zamawiający wymaga dostarczenia zewnętrznego narzędzia do deduplikowania replikowanych danych lub dwukrotnego zwiększenia pojemności ze względu na rozważaną w przyszłości replikację całości

zasobów. Macierz musi posiadać możliwość w ramach zaoferowanych licencji zaimplementowanie klastra geograficznego.

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 możliwość automatycznego informowania przez macierz i przesyłania przez pocztę elektroniczną raportów o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy.

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

8.12 Z macierzą zamawiający wymaga dostarczenia oprogramowania, które pozwala na:

8.12.1 monitoring wykorzystania przestrzeni na macierzy

8.12.2 monitoring grup RAIDowych

8.12.3 monitoring wykonywanych backupów/replikacji danych między macierzami

8.12.4 monitoring wydajności macierzy

8.12.5 analizę i diagnozę spadku wydajności

8.13 Zamawiający dopuszcza zastosowanie oprogramowania zewnętrznego, na pełną max pojemność macierzy.

8.14 Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy

8.15. Producent musi dostarczyć usługę w postaci portalu WWW lub dodatkowego oprogramowania umożliwiającą następujące funkcjonalności:

8.15.1 Narzędzie do tworzenia procedury aktualizacji oprogramowania macierzowego.

- procedura musi opierać się na aktualnych danych pochodzących z macierzy oraz najlepszych praktykach producenta.

- procedura musi uwzględniać systemy zależne np. macierze replikujące

- procedura musi umożliwiać generowanie planu cofnięcia aktualizacji.

8.15.2 Wyświetlanie statystyk dotyczących wydajności, utylizacji, oszczędności uzyskanych dzięki funkcjonalnościom macierzy.

8.15.3 Wyświetlanie konfiguracji macierzy oraz porównywanie jej z najlepszymi praktykami producenta w celu usunięcia błędów konfiguracji.

8.16 Portal lub oprogramowanie może pochodzić od innego producenta niż producent macierzy, z tym że zostanie dostarczona odpowiednia licencja do maksymalnej pojemności macierzy.

8.17 Zamawiający wymaga by wszystkie funkcjonalności działały wspólnie tj. włączenie jednej funkcjonalności nie eliminowało innej.

9. Gwarancja

9.1 serwis gwarancyjny, w tym producenta z 2 godzinnym czasem odpowiedzi na awarie krytyczne i dostawą elementów w na następny dzień roboczy

9.2 Dostarczony system musi posiadać również 2 lata subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia.

[Ochrona sondą XDR jak Managed Service]

50 szt. licencji oprogramowania antywirusowego

Zamawiający wykorzystuje obecnie oprogramowanie antywirusowe Eset Protect Entry 50 stanowisk o numerze klienta IP 33B-5VH-7JW, należy dostarczyć przedłużenie 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:
   - 1.1. Dostęp do subskrypcji aktualnych baz sygnatur.
   - 1.2. Dostęp do najnowszej wersji oprogramowania.
   - 1.3. 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 Debian, RedHat, 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.