Załącznik nr 1
Szczegółowy opis przedmiotu zamówienia

AKTUALIZACJA

Gmina Międzyrzec Podlaski
październik 2024

Spis treści

1. Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

- całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
- całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;

2. Równoważność

W przypadku użycia w dokumentacji opisującej przedmiot zamówienia odniesień do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych Zamawiający dopuszcza rozwiązania równoważne opisywanym. Wykonawca analizując dokumentację powinien założyć, że każdemu odniesieniu użytemu w dokumentacji towarzyszy wyraz „lub równoważne".
W przypadku, gdy w dokumentacji opisującej przedmiot zamówienia zostały użyte znaki towarowe, oznacza to, że są podane przykładowo i określają jedynie minimalne oczekiwane parametry jakościowe oraz wymagany standard. Wykonawca może zastosować materiały lub urządzenia równoważne do podanych znakiem towarowym (o ile dotyczy), lecz o parametrach technicznych i jakościowych podobnych (równych) lub lepszych, których zastosowanie w żaden sposób nie wpłynie negatywnie na prawidłowe funkcjonowanie rozwiązań przyjętych w dokumentacji. Wykonawca, który zastosuje urządzenia lub materiały równoważne będzie obowiązany wykazać w trakcie realizacji zamówienia, że zastosowane przez niego urządzenia i materiały spełniają wymagania określone przez Zamawiającego.
Użycie w dokumentacji opisującej przedmiot zamówienia etykiety oznacza, że Zamawiający akceptuje wszystkie etykiety potwierdzające, że dane dostawy spełniają równoważne wymagania określonej przez Zamawiającego etykiety.

3. Wymagania gwarancyjne.

Sprzęt

- o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona gwarancja; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
- Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Wnioskodawcy), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
- Gwarantowany czas naprawy nie może być dłuższy niż 10 dni roboczych. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
- Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Wnioskodawcy;
- wszystkie dostarczane moduły muszą pochodzić od producenta urządzeń i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu;

Oprogramowanie

- oprogramowanie powinno posiadać gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej);

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części SOPZ.

4. Miejsce instalacji sprzętu i oprogramowania/systemu.

- Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części dokumentu, w budynkach urzędu lub budynkach jednostek podległych, w miejscach wskazanych przez Zamawiającego.

5. Zestawienie zakresu dostaw i usług.

Lp.	Nazwa	Wymagana minimalna długość gwarancji (m-ce)	Ilość	Jednostka miary	Uwagi
1.	Serwer z oprogramowaniem	36	2	Szt.	Pozycja dotyczy stworzenie klastra niezawodnościowego HA, chmury prywatnej z dwóch fizycznych serwerów.
2.	Macierz dyskowa	36	1	Szt.	Pozycja dotyczy zakupu macierzy dyskowej w celu zapewnienia przestrzeni dyskowej dla klastera serwerów HA, który zostanie do niej podłączony.
3.	Oprogramowanie do backupu	24	1	Szt.	Na dedykowanym serwerze zostanie zainstalowane oprogramowanie do backupuZp i archiwizacji danych. System zostanie podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych. Miejscem przechowywania danych backupu będą dyski serwer. Połowa zasobów zostanie wykorzystana do przechowywanych plików off-line. Natomiast druga część zasobu zostanie wykorzystana do wykonywania replikacji asynchronicznej on-lina maszyn wirtualnych na lokalna platformę wirtualizacyjną na serwerze backupu.
4.	Firewall	24	1	Szt.	Pozycja dotyczy stworzenie klastra firewall, poprzez dołożenie drugiego urządzenia, który zabezpieczy punkt styku z Internetem, będzie terminował połączenia VPN z lokalizacji zdalnych, zapewni dostęp do zasobów sieciowych zgromadzonych w oprogramowani dziedzinowym oraz modułach świadczących e-usługi publiczne (wydzielenie sieci DMZ). Ruch z sieci VLAN zostanie zagregowany na tym urządzeniu. W ramach projektu zostaną opracowane polityki bezpieczeństwa dla ruchu sieciowego.
5.	Centralny system logów	24	1	Szt.	Pozycja pozwoli na zapisywanie i raportowanie zdarzeń w ruchu sieciowym z klastra firewall.
6.	Serwer backup	36	1	Szt.	Pozycja dotyczy elementu systemu kopii zapasowych. Obecny system nie pozwala na łatwe odzyskanie środowiska produkcyjnego oraz na utrzymanie ciągłości pracy. Konieczne jest zatem stworzenie dedykowanego systemu odmiejscowionej kopii zapasowej pozwalającego na odtworzenie kompletnego systemu. Na dedykowanym serwerze zostanie zainstalowane oprogramowanie do backupu i archiwizacji danych. System zostanie podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych. Miejscem przechowywania danych backupu będą dyski serwer. Połowa zasobów zostanie wykorzystana do

					przechowywanych plików off-line. Natomiast druga część zasobu zostanie wykorzystana do wykonywania replikacji asynchronicznej on-lina maszyn wirtualnych na lokalna platformę wirtualizacyjną na serwerze backupu.
7.	Przełącznik sieci LAN CORE	Wieczysta (Life time)	2	Szt.	Urządzenia pozwolą na stworzenie rozległej sieci szkieletowej 10G. Będą stanowiły centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI–L2 (warstwa łącza danych) oraz zapewnią wsparcie dla protokoły STP (protokół drzewa rozpinającego). Na przełącznikach zostanie zrealizowany mechanizm sieci wirtualnych VLAN (separacji ruchu sieciowego na warstwie L2 modelu ISO/OSI). Przełączniki zostaną połączone pomiędzy sobą z wykorzystaniem portów 10G SFP (w tym druga lokalizacja dla odmiejscowionego backupu) do lokalizacji głównej.
8.	System EDR-XDR	24	47	Szt.	Zakup pozwoli na zabezpieczenie punktów końcowych sieci. Będzie monitorował i gromadził dane z punktów końcowych sieci, a następnie używał tych informacji do wykrywania, badania i reagowania na różne zagrożenia bezpieczeństwa.
9.	System NAC	24	1	Szt.	Zakup pozwali na implementację protokołu 802.1x na przełącznikach sieci LAN i stacjach roboczych wraz integracją z usługa katalogową (domeną AD).
10.	Oprogramowanie do zarządzania siecią	24	1	Szt.	Pozwoli na konsoliduje wszystkich funkcji niezbędnych do zarządzania całą infrastrukturą IT w zakresie: monitorowania urządzeń, inwentaryzacji sprzętu i oprogramowania, użytkowników– zarządzanie dostępami, pomoc zdalna, bezpieczeństwa IT.
11.	Instalacja, konfiguracja, wdrożenie, utrzymanie.	24	1	Szt.	Pozycja dotyczy pełnej instalacji i konfiguracji dostarczonych elementów projektu (sprzętowo-programowych) wraz z migracja danych, przeszkoleniem administratorów urzędu oraz zapewnieniem wsparcia powdrożeniowego na okres trwania gwarancji (zgodnie z okresem wymaganym w SWZ i wskazanym w ofercie przez Wykonawcę).

6. Szczegółów opis pozycji.

6.1. Serwer z oprogramowaniem – szt. 2 – wymagania minimalne

Obudowa

- Typu RACK, wysokość 2U;
- Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
- Możliwość zainstalowania 16 dysków twardych hot plug 2,5”;
- Zainstalowane fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
- Zainstalowane 2 szt. dysków SSD 240GB skonfigurowane w RAID podpięte do sprzętowego kontrolera;
- Możliwość zainstalowania dysku M.2 NVMe PCIe4.0 x4;
- Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.
- Możliwość zainstalowania dedykowanego wewnętrznego napędu LTO-8.

Płyta główna

- Dwuprocesorowa;
- Wyprodukowana i zaprojektowana przez producenta serwera;
- Możliwość instalacji procesorów 60-rdzeniowych;
- Zainstalowany moduł TPM 2.0;
- 6 złącz PCI Express generacji 5 w tym:
  - 4 fizyczne złącza o prędkości x16;
  - 2 fizyczne złącza o prędkości x8;
  - Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
  - Opcjonalnie możliwość uzyskania 9 aktywnych interfejsów PCI-e;
- 32 gniazda pamięci RAM;
- Obsługa minimum 8 TB pamięci RAM DDR5;
- Wsparcie dla technologii:
  - Memory Scrubbing;
  - SDDC;
  - ECC;
  - Memory Mirroring;
  - ADDDC;
- Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.

Procesory

- Dwa procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86_64;
- Osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 246 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany w konfiguracji dwuprocesorowej dla dowolnego producenta serwera na stronie http://spec.org/cpu2017/results/cpu2017.html.

Pamięć RAM

- 256 GB pamięci RAM;
- DDR5 Registered 4800MT/s;
- Pamięci obsadzone w sposób gwarantujący najwyższa możliwość wydajność;

Kontrolery LAN

Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:

- 1x 1Gbit Base-T;
- 2x 10Gbit SFP+ obsadzone wkładkami MMF LC.
- Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

Kontrolery I/O

- Kontroler FC 2 x 16Gb

Porty

- Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
- 1 porty USB 3.0 wewnętrzne;
- 2 porty USB 3.0 dostępne z tyłu serwera;
- 2 porty USB 3.0 na panelu przednim;

- Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
- Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

Zasilanie, chłodzenie

- Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W;
- Redundantne wentylatory hotplug.

Zarządzanie

- Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;
    - informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
        - karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;
        - procesory CPU;
        - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
        - status karty zarządzającej serwera;
        - wentylatory;
        - bateria podtrzymująca ustawienia BIOS płyty głównej;
        - zasilacze;
        - system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);
- Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
    - Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
    - Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
    - Dostęp poprzez przeglądarkę Web, SSH;
    - Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
    - Zarządzanie alarmami (zdarzenia poprzez SNMP);
    - Możliwość przejęcia konsoli tekstowej;
    - Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
    - Obsługa serwerów proxy (autentykacja);
    - Obsługa VLAN;
    - Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
    - Wsparcie dla protokołu SSDP;
    - Obsługa protokołów TLS 1.2, SSL v3;
    - Obsługa protokołu LDAP;
    - Integracja z HP SIM;
    - Synchronizacja czasu poprzez protokół NTP;
    - Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;
- Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
- Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;
- Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
- Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

Wspierane OS

- Microsoft Windows Server 2022, 2019;
- VMWare vSphere 8.0;
- Suse Linux Enterprise Server 15;
- Red Hat Enterprise Linux 9, 8;
- Microsoft Hyper-V Server 2019.

Gwarancja

- 3 lata gwarancji serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.
- Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych lub równoważny;
- Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
- Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki.

Dokumentacja, inne

- Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta,;
- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera;
- W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
- Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 85 %;
- Zgodność z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych (Dyrektywa delegowana komisji (UE) 2015/863 z dnia 31 marca 2015 r. zmieniająca załącznik II do dyrektywy Parlamentu Europejskiego i Rady 2011/65/UE).

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz umożliwiać zainstalowanie minimum 1000 instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. 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.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.

9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
   b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Mechanizmy logowania w oparciu o:
   a. Login i hasło,
   b. Karty z certyfikatami (smartcard),
   c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
   a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
   b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
      - Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
      - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
      - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
      - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
   c. Zdalna dystrybucja oprogramowania na stacje robocze.
   d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
   e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
      - Dystrybucję certyfikatów poprzez http
      - Konsolidację CA dla wielu lasów domeny,
      - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
      - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f. Szyfrowanie plików i folderów.
g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
i. Serwis udostępniania stron WWW.
j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
k. Wsparcie dla algorytmów Suite B (RFC 4869),
l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
    - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
    - Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
    - Obsługi 4-KB sektorów dysków
    - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
    - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
    - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

6.2. Macierz dyskowa – szt. 1 – wymagania minimalne

Ogólne

System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzewodową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii. Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy lub musi być dostarczona licencja na dwukrotność dostarczanej pojemności. Dostarczana macierz musi umożliwiać takie podłączenie półek, aby awaria lub/i usunięcie jednej z półek nie powodowało utraty dostępu do danych znajdujących się na pozostałych modułach. Oferowana macierz musi obsługiwać min. 142 dyski wykonane w technologii hot-plug. Wszystkie zainstalowane dyski hot-plug, z wyłączeniem dysków SSD stosowanych jako rozszerzenie pamięci Cache kontrolerów, muszą być dostępne dla zapisu danych Użytkownika. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów (tzw. „półek dyskowych”) w rozmiarze 2U pozwalająca umieścić do 24 dysków 2,5” typu hotplug dla dysków SAS i SSD oraz w rozmiarze 2U dla 12 dysków 3,5” typu hotplug NL-SAS i SSD. Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych (tj. 2,5” + 3,5”).

Pojemność macierzy:

18 szt. dysków twardych SSD-SAS o pojemności 1,92TB każdy;

Kontrolery

Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi 2 kontrolerami;

Każdy z kontrolerów macierzy musi posiadać po16GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu;
Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o 800GB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD,
W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk.
Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia;
Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach.
Każdy z kontrolerów RAID powinien posiadać dedykowany minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.
Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej.
Kontrolery macierzy muszą obsługiwać do 70 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów
Oferowana macierz musi mieć wyprowadzone 4 porty FC 16Gb/s do dołączenia serwerów bezpośrednio lub do sieci san na każdy kontroler RAID.
Macierz musi umożliwiać wymianę połowy portów do transmisji danych dla każdego z kontrolerów na:

- 2x FC 32 Gb/s,
- 2x iSCSI Base-T,
- 2x SAS 12Gb/s,
- 2x iSCSI SFP+,

Wymiana portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych
Macierz posiada obsługę operacji plikowych I/O w sieci NAS w obrębie zainstalowanych kontrolerów. Protokoły dostępu: CIFS, NFS. W przypadku obsługi protokołów CIFS i NFS wymagana jest funkcjonalność agregacji przepustowości dla interfejsów dedykowanych do obsługi tych protokołów. Obsługa protokołów CIFS i NFS musi odbywać się jednocześnie. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy

Poziomy RAID

Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:

- Raid-1
- Raid-10
- Raid-5
- Raid-50
- Raid-6

Dyski

Oferowana macierz musi wspierać dyski hot-plug:

- dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s
- dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm,

Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania;
Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex
Macierz musi obsługiwać min. 140 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami;
Możliwość rozbudowy oferowanego modelu macierzy do 520 dysków bez migracji i przenoszenia danych - jedynie poprzez wymianę modułu kontrolerów macierzy (bez konieczności wymiany posiadanych dysków, półek dyskowych, bez konieczności przenoszenia danych/ istniejącej struktury grup dyskowych/LUN, jak również z zachowaniem istniejącej gwarancji na półki dyskowe i dyski;
Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) lub wirtualna przestrzeń zapasowa:

- Macierz posiada możliwość konfiguracji dysku hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID
- Macierz posiada możliwość konfiguracji dysku hot-spare dedykowanego dla zabezpieczenia tylko wybranej grupy dyskowej RAID

W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na

wymieniony dysk (tzw. CopyBackLess) lub nie wymaga zwolnienia zapasowej przestrzeni wirtualnej.
Macierz musi pozwalać na zaszyfrowanie danych zapisanych na wszystkich obsługiwanych dyskach SSD-SAS, HDD-SAS oraz HDD NL-SAS minimum kluczem AES256-bit dla danych blokowych – jeżeli w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą.
Macierz musi umożliwiać zaszyfrowanie całej dostępnej powierzchni użytkowej minimum kluczem AES256-bit.
Opcje programowe
Macierz musi być wyposażona w system umożliwiający wykonanie kopii migawkowych
Macierz musi umożliwiać zdefiniowanie 4000 woluminów (LUN)
Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez 1000 ścieżek logicznych FC
Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów
Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową
Macierz musi posiadać wsparcie dla systemów operacyjnych : Microsoft Windows Server 2012R2, 2016, 2019, SuSE Linux Enterprise Server, Red Hat Linux Enterprise Server, HP-UNIX, IBM AIX, SUN Solaris, Vmware Vsphere;
Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.
Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy;
Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy;
Macierz musi obsługiwać mechanizm ochrony priorytetów obsługi wybranych zasobów – za taki mechanizm uznaje się funkcję typu ‘cache partitioning’ lub ‘storage partitioning’.
Macierz musi obsługiwać adresację IP v.4 i IP v.6
Wraz z macierzą należy dostarczyć oprogramowanie lub moduły programowe typu plug-in pozwalające na integracje macierzy w środowiskach Vmware w zakresie obsługi mechanizmów: Vmware VAAI, Vmware VVOL, Vmware MultiPath IO – z subskrypcją do bezpłatnej aktualizacji w całym okresie obowiązywania gwarancji
Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy.
Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SAS, NL-SAS. Macierz musi pozwalać na definiowanie różnych polityk i zasad migrowania danych w obrębie tej samej macierzy. Mechanizm AST musi pozwalać na definiowanie okna czasowego dla zbierania pomiarów wydajności operacji I/O oraz okna czasowego dla migrowania danych wg ustalonych zasad i polityk – minimalny definiowany czas trwania w/w operacji (długość okna czasowego) nie może być dłuższy niż 4 godziny. Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy
Mechanizm AST musi być obsługiwać funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) mierzonej jako maksymalny czas opóźnień operacji I/O wykonywanych przez serwer/środowisko/aplikację. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy
Macierz musi wspierać usługi VSS (Volume ShadowCopy Services) w systemach klasy Microsoft Windows Sever – wymagane jest dostarczenie niezbędnego oprogramowania / sterowników VSS pozwalających na obsługę VSS przy maksymalnej pojemności i liczbie dysków obsługiwanych przez oferowaną. W czasie trwania gwarancji wymaga się bezpłatnego dostępu do nowych wersji oprogramowania i sterowników

Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy tej klasy, z zachowaniem obsługi operacji I/O dla serwerów podłączonych do migrowanej macierzy tj. do migrowanych zasobów LUN

Macierz wspiera rozwiązania klasy 'klastra macierzowego' tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software'owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami protokołami FC oraz iSCSI. Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC oraz iSCSI, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy. Pod użytym pojęciem 'wysoka dostępność zasobów dyskowych' należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzą, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Funkcjonalność 'klastra macierzowego' musi pozwalać na automatyczne i ręczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. Automated/manual failover). – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy

Zarządzanie

Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej

Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.

Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora

Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI

Należy dostarczyć i wstępnie skonfigurować system zarządzania infrastrukturą IT. Musi być możliwość monitorowania stanu środowiska IT minimum dla oferowanej macierzy oraz serwerów. System zarządzania posiada jeden spójny interfejs GUI HTML do zarządzania oferowanym środowiskiem sprzętowym. System zarządzania opiera się o tzw. Virtual Appliance kompatybilny z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM. System zarządzania umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe. System zarządzania posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI. System zarządzania musi mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV.

Gwarancja i serwis

Całe rozwiązanie musi być objęte 36 miesięcznym okresem gwarancji z naprawą miejscu instalacji urządzenia i z gwarantowaną wizytą technika do końca następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy. Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej.

Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego.

Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy oraz do kolejnych wersji oprogramowania zarządzającego w okresie minimum 2 lat.

System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół. Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta.

Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych

Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia

Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty);

Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia

gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia.

6.3. Oprogramowanie do backupu – szt. 1 – wymagania minimalne

Wymagania ogólne

- Minimalna ilość licencji musi umożliwiać backup środowiska wirtualnego z co najmniej dwóch serwerów 2-procesorowych obejmującego co najmniej 20 VM oraz 3 serwerach fizycznych.
- Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
- Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
- Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
- Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Całkowite koszty posiadania

- Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
- Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
- Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
- Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
- Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
- Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
- Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
- Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
- Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
- Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
- Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
- Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
- Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
- Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Wymagania RPO

- Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
- Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

- Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
- Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
- Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
- Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
- Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
- Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
- Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
- Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
- Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)
- Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
- Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
- Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
- Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

Wymagania RTO

- Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
- Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
- Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
- Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
- Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
- Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
- Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
  - Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
  - BSD: UFS, UFS2
  - Solaris: ZFS, UFS
  - Mac: HFS, HFS+
  - Windows: NTFS, FAT, FAT32, ReFS
  - Novell OES: NSS
- Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.

- Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
- Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
- Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
- Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
- Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
- Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
- Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
- Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
- Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka

- Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
- Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
- Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
- Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
- Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Monitoring

- System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
- System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
- System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware
- System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
- System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
- System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
- System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
- System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora

- System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
- System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
- System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
- System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
- System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
- System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
- System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
- System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 9.x i 10.x

Raportowanie

- System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022
- System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
- System musi być certyfikowany przez VMware i posiadać status „VMware Ready”
- System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
- System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
- System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
- System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
- System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
- System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
- System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
- System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
- System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
- System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
- System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
- System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
- System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
- System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

6.4. Firewall – szt. 1 – wymagania minimalne

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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.

System musi wspierać IPv4 oraz IPv6 w zakresie:

1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 128 GB.
5. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.
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 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.

- Policy Based Routingu.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek

takich jak: Google, oraz Yahoo.

6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

6.5. Centralny system logów – szt. 1 – wymagania minimalne

Wymagania Ogólne

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Interfejsy, Dysk:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 500 GB

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 1 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 100 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
   a. Listę najczęściej wykrywanych ataków.
   b. Listę najbardziej aktywnych użytkowników.
   c. Listę najczęściej wykorzystywanych aplikacji.
   d. Listę najczęściej odwiedzanych stron www.
   e. Listę krajów , do których nawiązywane są połączenia.
   f. Listę najczęściej wykorzystywanych polityk Firewall.
   g. Informacje o realizowanych połączeniach IPSec.
4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   - Malware.
   - Aplikacje sieciowe.

- Email.
- IPS.
- Traffic.
- Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje

1. Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

6.6. Serwer backup – szt. 1 – wymagania minimalne

Obudowa

- Typu RACK, wysokość 2U;
- Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
- Możliwość zainstalowania 12 dysków twardych hot plug 3,5”;
- Zainstalowane fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
- Zainstalowane 2 szt. dysków SSD 1,92TB Hot-Plug DWPD>2
- Zainstalowane 10 szt. dysków SAS lub NL-SAS 12G 12TB Hot-Plug skonfigurowane w RAID podpięte do sprzętowego kontrolera;
- Możliwość zainstalowania dysku M.2 NVMe PCIe4.0 x4;

Płyta główna

- Dwuprocesorowa;
- Wyprodukowana i zaprojektowana przez producenta serwera;
- Możliwość instalacji procesorów 60-rdzeniowych;
- Zainstalowany moduł TPM 2.0;
- 6 złącz PCI Express generacji 5 w tym:
  - 4 fizyczne złącza o prędkości x16;
  - 2 fizyczne złącza o prędkości x8;
  - Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
  - Opcjonalnie możliwość uzyskania 9 aktywnych interfejsów PCI-e;
- 32 gniazda pamięci RAM;
- Obsługa minimum 8 TB pamięci RAM DDR5;
- Wsparcie dla technologii:
  - Memory Scrubbing;
  - SDDC;
  - ECC;
  - Memory Mirroring;
  - ADDDC;
- Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) dyski nie mogą zajmować klatek dla dysków hot-plug.

Procesory

- Dwa procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86_64;
- Osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 246 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany w konfiguracji dwuprocesorowej dla dowolnego producenta serwera na stronie http://spec.org/cpu2017/results/cpu2017.html.

Pamięć RAM

- 256 GB pamięci RAM;
- DDR5 Registered 4800MT/s;

Kontrolery LAN

Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:

- 1x 1Gbit Base-T;
- 2x 10Gbit SFP+, wszystkie porty obsadzone modułami MMF LC;
- Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

Kontrolery I/O

- Kontroler SAS RAID dla dysków wewnętrznych posiadający 4GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania;

Porty

- Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
- 1 porty USB 3.0 wewnętrzne;
- 2 porty USB 3.0 dostępne z tyłu serwera;
- 2 porty USB 3.0 na panelu przednim;
- Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
- Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

Zasilanie, chłodzenie

- Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W;
- Redundantne wentylatory hotplug.

Zarządzanie

- Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;
    - informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
        - karty rozszerzeń zainstalowane w dowolnym slocie PCI Express;
        - procesory CPU;
        - pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
        - status karty zarządzającej serwera;
        - wentylatory;
        - bateria podtrzymująca ustawienia BIOS płyty głównej;
        - zasilacze;
        - system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);
- Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
    - Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
    - Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
    - Dostęp poprzez przeglądarkę Web, SSH;
    - Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
    - Zarządzanie alarmami (zdarzenia poprzez SNMP);
    - Możliwość przejęcia konsoli tekstowej;
    - Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
    - Obsługa serwerów proxy (autentykacja);
    - Obsługa VLAN;
    - Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
    - Wsparcie dla protokołu SSDP;
    - Obsługa protokołów TLS 1.2, SSL v3;
    - Obsługa protokołu LDAP;
    - Integracja z HP SIM;
    - Synchronizacja czasu poprzez protokół NTP;

- Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;
- Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
- Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;
- Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
- Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

Wspierane OS

- Microsoft Windows Server 2022, 2019;
- VMWare vSphere 8.0;
- Suse Linux Enterprise Server 15;
- Red Hat Enterprise Linux 9, 8;
- Microsoft Hyper-V Server 2019.

Gwarancja

- 3 lata gwarancji serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej;
- Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych lub równoważny;
- Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
- Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).

Dokumentacja, inne

- Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;
- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;
- W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
- Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 85 %;
- Zgodność z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych (Dyrektywa delegowana komisji (UE) 2015/863 z dnia 31 marca 2015 r. zmieniająca załącznik II do dyrektywy Parlamentu Europejskiego i Rady 2011/65/UE).

6.7. Przełącznik sieci LAN Core – szt. 2 - wymagania minimalne

Przełącznik wielowarstwowy L2/L3, zarządzany

Typ i liczba portów: 12 portów 10GBaseT i 12 portów SFP+ lub równoważnie 24 poty SFP+

Porty SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:
- Gigabit Ethernet 1000Base-SX
- Gigabit Ethernet 1000Base-LX/LH
- 10Gigabit Ethernet 10GBase-SR
- 10Gigabit Ethernet 10GBase-LR
- 10Gigabit Ethernet typu twinax

Port konsoli USB Type-C/RJ45
Porty dostępowe przełącznika zgodne ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)

Parametry wydajnościowe:
- Przepustowość przełącznika (switching bandwidth) 480 Gb/s
- Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów 240 Mpps
- Pamięć DRAM – 512 MB
- Pamięć flash – 256 MB
- Procesor wbudowany 1,3 GHz
- Wielkość bufora pakietów - 3 MB
- 2 000 grup IGMP
- 8 grupy połączeń zagregowanych typu „port channel" LACP
- 8 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP
- 1 000 wpisów w listach kontroli dostępu ACL
- 8 kolejek sprzętowych

Obsługa:
- 4 090 aktywnych sieci VLAN
- 16 000 adresów MAC
- 900 statycznych tras IPv4
- 128 interfejsów L3

Obsługa ramek Ethernet Jumbo 9 000 B

Możliwość łączenia do 4 jednostek w stos poprzez porty 10 GE, zarządzane jako jeden system z funkcją failover active/standby
Funkcjonalność cross-stack QoS, VLAN, LAG i port mirroring

Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
- IEEE 802.1w Rapid Spanning Tree
- Per-VLAN Rapid Spanning Tree (PVRST+)
- IEEE 802.1s Multi-Instance Spanning Tree
- Obsługa 126 instancji protokołu STP

Funkcje wirtualnej sieci LAN: Voice VLAN, Protocol based VLAN
Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
Protokół rejestracji GARP VLAN (GVRP)

Mechanizmy związane z bezpieczeństwem sieci:
- Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level)
- Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
- Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
- Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
- Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
- Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
- Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i

TACACS+,
- Obsługa HTTPS, SSH, SSL
- Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP)

Mechanizmy związane z zapewnieniem jakości usług w sieci:
- Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
- Implementacja algorytmu Weighted Round Robin dla obsługi kolejek
- Możliwość obsługi jednej z kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
- Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
- Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi,
- Kontrola sztormów dla ruchu broadcast/multicast/unicast
- Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP

Obsługa standardów komunikacyjnych:
IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbit/s Ethernet over fiber for LAN, IEEE 802.3an 10GBase-T 10 Gbit/s Ethernet over copper twisted pair cable, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient Ethernet

Obsługa protokołu NTP
Funkcje DHCP server, DHCP relay
Obsługa IGMPv1/2/3 i MLDv1/2 Snooping, DHCP snooping
Blokowanie Head of Line (HOL)

Zabezpieczenie przed wejściem w pętlę Unidirectional Link Detection (UDLD)
Zapobieganie atakom DoS

Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6
Routing dynamiczny RIP v2

Zarządzanie
- Port konsoli
- Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją
- Obsługa protokołów SNMPv3, SSHv2, https, syslog
- Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia
- Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki
- Obsługa protokołu LLDP i LLDP-MED

Obsługa funkcji Plug & Play
Przycisk reset
Zasilanie 230V AC
Wysokość maksymalnie 1U, montowany w szafie typu RAC 19''

6.8. System EDR-XDR – szt. 47 – wymagania minimalne

Administracja zdalna

1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.

2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
7. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
8. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).
9. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
10. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
11. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
12. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
13. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
14. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
15. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS,

POP3S, IMAPS.

13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
    - tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    - tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
    - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera

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

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie

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

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
   - usunięcie zawartości urządzenia,
   - przywrócenie urządzenie do ustawień fabrycznych,
   - zablokowania urządzenia,
   - uruchomienie sygnału dźwiękowego,
   - lokalizację GPS.
6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
   - nazwę aplikacji,
   - nazwę pakietu,
   - kategorię sklepu Google Play,
   - uprawnienia aplikacji,
   - pochodzenie aplikacji z nieznanego źródła.

Sandbox w chmurze

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

Moduł XDR

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego

samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica".
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
16. Konsola administracyjna musi mieć możliwość tagowania obiektów.
17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

6.9. System NAC – szt. 1 – wymagania minimalne

Podstawowa funkcjonalność systemu:

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 250 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 50000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.

9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
    - VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x
    - Maszyny fizyczne - serwery wspierane przez producenta.
11. System musi posiadać funkcjonalność serwerów:
    - serwera RADIUS dla infrastruktury sieciowej,
    - serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
    - serwera SYSLOG,
    - serwera TACACS+,
    - serwera Monitoringu,
    - serwera DHCP,
    - serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
    - serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now.
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji

urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.
59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni

sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:

- Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
- Czy włączony jest firewall
- Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
- Czy jest włączone szyfrowanie dysku systemowego
- Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
- Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
- Czy w systemie są uruchomione procesy wskazane przez administratora
- Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
- Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
  - Wartości klucza rejestru
  - Typu wartości: Number, String, Version

60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
61. System musi współpracować z serwerem tokenów.
62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:
    - Microsoft Windows
    - Mac OS
    - iOS
    - Android
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

Mechanizmy uwierzytelniania

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
    - MAC,
    - PAP/ASCII,
    - CHAP,
    - SNMP,
    - 802.1X.
3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.
4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
    - Tożsamość/Urządzenie końcowe,
    - Grupa tożsamości/urządzeń końcowych,
    - Parametry urządzeń końcowych, min: system operacyjny, wersja,
    - Atrybuty Active Directory,
    - Jednostka organizacyjna tożsamości/urządzeń końcowych,
    - Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
    - Grupy urządzeń sieciowych,
    - Porty urządzeń sieciowych,
    - Grupy portów urządzeń sieciowych,
    - Jednostka organizacyjna portów,
    - Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
    - Data, czas ważności polityki,

- Wewnętrzny Captive Portal,
- Metoda autoryzacji.

8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
19. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
20. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
21. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

Obsługa serwerów certyfikatów CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
   - możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
   - możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
   - Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
   - usługę OCSP (Online Certificate Status Protocol).

Obsługa serwerów DHCP

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
   - Uruchamianie usługi dla wybranych podsieci,
   - Przypisanie ustalonego adresu IP dla adresu MAC.
   - Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
   - Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
   - Możliwość określania braku dostępu dla wybranych adresów MAC,
   - Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla

zdefiniowanej grupy adresów MAC,
- Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
- Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
- Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
- Dokonywanie zmian bez konieczności wyłączania usług.

Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.

Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadam adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum:
    - Logowania, wylogowania z system w tym błędne logowania
    - Logowania do sieci 802.1X

Alarmy

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
    - wiadomości e-mail,
    - Syslog,
    - notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min:
    - Ilości obsługiwanych transakcji RADIUS,

- Opóźnienie obsługi transkacji RADIUS,
- Statusu krytycznego modułów.

3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
   - badanie łączności IP za pomocą ping, traceroute,
   - tcpdump protokołów RADIUS, TACACS+,
   - wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
     - nazwy użytkownika,
     - adresu MAC,
     - statusu uwierzytelnienia (udana lub nieudana),
     - powodu, jeżeli uwierzytelnienie nieudane,
     - zakresu czasowego, co do dnia, godziny i minuty,
   - wykonanie zdalnego polecenia na urządzeniu sieciowym.

6.10. Oprogramowanie do zarzadzania siecią – szt.1 – wymagania minimalne.

1. Architektura / budowa
   - 1.1. Licencja bezterminowa na oprogramowanie powinna objąć wszystkie stanowiska komputerowe z 24 miesięcznym wsparciem serwisowym.
   - 1.2. System musi posiadać następującą architekturę:
     - 1.2.1. Agent – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
     - 1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych).
     - 1.2.3. Panel pracownika – aplikacja webowa dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej.
     - 1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z agentami.
     - 1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.
     - 1.2.6. Komponenty Agent, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja agentów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie ze strony producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.
     - 1.2.7. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, pakietów, pomoc i inne wbudowane bazy wiedzy.
     - 1.2.8. Agent do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI.
     - 1.2.9. Agent musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku msi.
     - 1.2.10. Agent musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej.
     - 1.2.11. System musi posiadać możliwość wygenerowania instalatora Agenta, który nie będzie wymagał uprawnień administracyjnych do zainstalowania.
     - 1.2.12. Agent musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa).

1.2.13. System powinien umożliwiać generowanie unikatowego identyfikatora agenta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków.

1.2.14. Agent musi mieć definiowalny priorytet pracy (ABOVE_NORMAL, NORMAL, BELOW_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów.

1.2.15. Agent musi wspierać do sześciu różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu agenta.

1.2.16. System musi umożliwiać komunikację pomiędzy agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.

1.2.17. System musi mieć możliwość współpracy komponentów agent i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami agentów.

1.2.18. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem realizujące co najmniej: usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nieprzyrostowe, zmniejszanie bazy danych. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie. System musi prezentować historię przeprowadzonych konserwacji/utrzymania.

2. Wymagania systemowe

2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, Firefox, Chrome, Opera).

2.2. Agent musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.

2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11.

2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2012/2012R2/2016/2019/2022, Windows 10) oraz Java 8 (JRE lub JDK), Apache Tomcat 8+.

2.5. Baza danych musi działać na silniku Microsoft SQL Server 2012/2014/2016/2017/2019 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).

2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

3. Interfejsy

1.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.

1.2. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.

1.3. Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS.

1.4. Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny.

1.5. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z dowolnego źródła danych o dowolnej strukturze danych z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane.

1.6. System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS.

4. Funkcjonalności systemu zarządzania infrastrukturą IT

4.1. Funkcjonalność agenta

4.1.1. System musi umożliwiać pełne zdalne zarządzanie agentami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania agenta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego), uruchamiania i wyłączania polityk w obszarze bezpieczeństwa (DLP).

4.1.2. Agent musi mieć możliwość konfiguracji zakresu skanowania plików w oparciu o nazwę plików (z uwzględnieniem znaków wieloznacznych), lokalizację na konkretnym dysku, datę utworzenia pliku oraz wielkość

4.1.3. Agent musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej a konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił.

4.1.4. Agent musi mieć budowę modułową – uniemożliwienie pracy jednego z modułów (np. w wyniku niekompatybilnego systemu operacyjnego, pracy programów firm trzecich, awarii sprzętowej) nie może blokować pracy całego Agenta.

4.1.5. Po wykryciu nieprawidłowości w pracy dowolnego z modułów Agent powinien podjąć samoczynną próbę jego naprawy i przywrócenia do działania.

4.2. Funkcjonalność konsoli administracyjnej.

4.2.1. Konsola musi być w pełni polskojęzyczna oraz dodatkowo posiadać wersje angielską.

4.2.2. Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie).

4.2.3. Konsola administracyjna musi posiadać dashboardy – dashboard użytkownika, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie.

4.2.4. Dashboard użytkownika jest budowany samodzielnie przez użytkownika poprzez wybór szybkiego skrótu do dowolnego ekranu aplikacji lub wybór dowolnego widgetu.

4.2.5. Dashboard prezentujący parametry sieci zawiera widgety pogrupowane w kategorie: Czat, Gry, Peer to peer, Streaming, Usługa podstawowa, Usługa podstawowa (szyfrowana), Złośliwe oprogramowanie.

4.2.5.1.1. Lista monitorowanych usług: AIM/ICQ, Back Orifice, Bagle.B, Bagle.h, BGMP, BGP, BitTorrent, Blaster, Blizzard's Battle.net, Call of Duty, Dabber, DHCPv6 (client), DHCPv6 (server), Direct Connect, DNS, Doom, Emule, FTP (connection control), FTP (data port), FTPS (TLS/SSL)(connection control), FTPS (TLS/SSL)(data port), GameSpy Arcade, Gnutella, Gopher protocol, HTTP, HTTP Proxy, HTTPS, IMAP, IMAPS, IMAPv3, iperf, IRC, IRC, iSCSI, Jedi Knight: Jedi Academy, Kazza, Kerberos, Killing Floor, LDAP, LDAP (SSL), LDP, LogMeIn Hamachi, MMP, MPP, MS Exchange Routing, MS Media Server, MS SQL Server (monitor), MS SQL Server (server), MSDP, MSN, Mu Online, Mxit, MySQL, Nessus, NetBIOS (Datagram Service), NetBIOS (Name Service), NetBIOS (Session Service), NetBus, NFS, Niektóre gry firmy Blizzard, Nintendo Wi-Fi Connection, NNTP, NNTP (TLS/SSL), NTP, OpenVPN, POP3, POP3S, PostgreSQL, PPTP, Printer-IPP, Printer-RAW, Print-spooler, Radio internetowe, Rbot/Spybot, RDP, rsyns, RTCP, RTP, RTSP, Sasser, SFTP, SIP, SIP(TLS), SLP, SMB, SMTP,SMTPS, SNMP, SOCKS proxy, SSH, Steam, Structured Query Language (SQL) Services, Sub7, Symantec System Center agent, TACACS, TeamViewier, Telenet (TLS/SSL), Telnet, TSP, UUCP, VMware Server, VMware VAMI, WASTE, WHOIS, WINS, XMPP/Jabber, Yahoo,! Messenger.

4.2.5.1.2. Dla każdej z usług prezentowane są relacje do wszystkich komputerów zawierające połączenia: powolne, nieosiągalne, rozłączone i poprawne wraz z czasami połączeń.

4.2.6. Dashboard prezentujący informacje o bezpieczeństwie zawiera widgety zawierające informacje: błędy serwera zadań, błędy smart, komputery bez bitlockera, komputery bez połączenia z serwerem, komputery z błędami typu critical / error / warning, duży transfer sieciowy, komputery bez agenta, komputery offline, komputery online, komputery z naruszoną polityką dlp, komputery z nieaktualną polityką dlp, liczba administratorów lokalnych w systemie (online), logowanie w godzinach nocnych, monitorowanie transferu do dysków chmurowych , nieautoryzowana pamięć usb, nowe komputery, nowe urządzenia w

sieci, oprogramowanie zabronione, przekroczone cal, przekroczone licencje, subskrypcje, które wygasły, systemy bez wsparcia, wielokrotne logowanie, wysokie użycie cpu, wysokie użycie ram, zaległe szkolenia wideo, zaległe wiadomości elearning, zbyt mało miejsca na hdd, zmiany na kontach użytkowników, zmiany tcp/ip.

4.2.7. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widgety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi.

4.2.8. Dane na widgetach muszą być aktualizowane automatycznie nie rzadziej niż 1 raz/ godzinę lub w każdym czasie na życzenia użytkownika.

4.2.9. Widgety muszą być skojarzone dziedzinowo ze wszystkimi obszarami zarządzania infrastrukturą, a każdy obszar powinien być reprezentowany przez min. 5 widgetów (np. w obszarze zarządzania komputerami system powinien być wyposażony w widgety zawierające: ilość komputerów w ramach danego typu, ilość komputerów on/off-line, strukturę komputerów wg ilości pamięci RAM, ilość komputerów wg ilości wolnego miejsca na dysku, ilość komputerów wg dat ostatnich połączeń)

4.2.10. Z każdego widgetu można uzyskać szczegółową informację analityczną (listę z danymi składającymi się na wybraną wartość na widgecie).

4.2.11. System musi posiadać filtr roboczy, przeszukujący całą tabelę po zdefiniowanym słowie.

4.2.12. System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widgety, ich konfigurację i kolejność).

4.2.13. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu. Reguły muszą być zapamiętywane i dostępne w kolejnych sesjach oraz oparte co najmniej o: nazwę komputera, IP, rodzaj systemu operacyjnego, identyfikator agenta, strukturę organizacyjną, stan agenta (włączony/wyłączony), nazwę użytkownika zalogowanego, producenta sprzętu, dostawcę sprzętu, lokalizację komputera, dowolnie zdefiniowaną przez użytkownika wartość (np. kolor obudowy komputera). Użytkownik może wybrać za jednym razem więcej niż jedną regułę. Zmiana wybranej reguły powoduje aktualizację wyświetlonego widoku.

4.2.14. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego.

4.2.15. System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, dodawanie, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.

4.2.16. Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu.

4.2.17. Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko).

4.2.18. Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja agenta, stanu agenta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.

4.2.19. Konsola musi umożliwić bezpośrednie przejście do witryny internetowej producenta z poziomu repozytorium producentów (o ile taka jest dostępna, np. DELL).

4.2.20. Konsola musi umożliwić bezpośrednie przejście do strony producenta zawierającej dodatkowe dane konfiguracyjne na temat konkretnego komputera w oparciu o Service Tag lub inny unikatowy identyfikator (np. Dell)

4.2.21. Konsola musi zawierać w sobie pełną dokumentację systemu, dokumentacja musi być na bieżąco aktualizowana poprzez automatyczne mechanizmy aktualizacji z serwera aktualizacji producenta.

4.3. Funkcjonalność panelu pracownika

4.3.1. Automatyczne uruchamianie panelu w momencie zalogowania użytkownika do systemu operacyjnego.

4.3.2. Zakres informacji w panelu jest definiowany przez administratora w formie schematów przypisywanych dla wybranych grup pracowników.

4.3.3. Panel pracownika użytkowany przez kierownika zawiera dodatkowo dane dostępne w panelach podległych pracowników w formie danych skumulowanych i analitycznych.
4.3.4. Wszelkie informacje udostępniane w panelu pracownika pogrupowane są w logiczne sekcje, z możliwością indywidulanego bądź grupowego włączania / wyłączania (ukrywania) sekcji.
4.3.5. Sekcje informacyjne panelu pracownika
4.3.5.1. Zalogowany użytkownik – imię i nazwisko, IP, nazwa komputera, informacje z AD – nazwa domenowa, nr telefonu, nr telefonu komórkowego, stanowisko
4.3.5.2. Dashboard
4.3.5.2.1. Mój komputer – wykorzystanie RAM, dysku, CPU.
4.3.5.2.2. Wiadomości – lista ostatnich wiadomości przesłanych pracownikowi.
4.3.5.3. Sprzęt
4.3.5.3.1. Komputery przypisane do pracownika (nr seryjny, MAC, IP, data ostatniego logowania).
4.3.5.3.2. Komputery używane przez pracownika (nr seryjny, MAC, IP, data ostatniego logowania).
4.3.5.3.3. Urządzenia przypisane przez pracownika (nr seryjny, typ, IP).
4.3.5.3.4. Urządzenia używane przez pracownika (nr seryjny, typ, IP).
4.3.5.4. Oprogramowanie
4.3.5.4.1. Lista używanego oprogramowania (nazwa aplikacji, wersja, Producent, użycie 2 okresi ostatnich 3, 6, 12 miesięcy, data ostatniego uruchomienia).
4.3.5.5. Wiadomości
4.3.5.5.1. Lista wiadomości przesłanych do użytkownika (data, typ wiadomości, nadawca, treść).

4.4. Zarządzanie licencjami
4.4.1. System musi umożliwiać zarządzanie licencjami w ramach dowolnego elementu struktury organizacyjnej (dla wybranej struktury organizacyjnej pokazuje liczbę instalacji i liczbę licencji w danym modelu licencjonowania wraz z listą komputerów).
4.4.2. System musi dawać możliwość wykonywania (historia) wielu audytów legalności i zapamiętywać wyniki tych audytów w odniesieniu do systemów operacyjnych jak i aplikacji/pakietów, z uwzględnieniem segmentu struktury organizacyjnej.
4.4.3. Zarządzanie oprogramowaniem musi następować z podziałem na aplikacje i pakiety oprogramowania.
4.4.4. System musi pozwalać na zdefiniowanie dowolnej ilości tzw. „standardów oprogramowania", które definiują 3 kategorie oprogramowania: „oprogramowanie standardowe" – pozycje z tej listy są wymagane do zainstalowania obowiązkowo na każdym komputerze, „oprogramowanie dodatkowe" - pozycje z tej listy mogą być zainstalowane (nie jest to wymagane) a instalacja odbywa się na wniosek samego użytkownika lub jego przełożonego, „oprogramowanie nieokreślone" – oprogramowanie nie należące do żadnej z dwóch powyżej zdefiniowanych kategorii a zidentyfikowane na komputerze.
4.4.5. System umożliwia zdefiniowanie listy aplikacji zabronionych.
4.4.6. System umożliwia utworzenie schematów (kolekcji) oprogramowania zabronionego i w momencie pojawienia się ich na komputerze przystępuje do automatycznego odinstalowania w trybie cichym (bez interfejsu).
4.4.7. System musi umożliwiać zdefiniowanie dowolnej kategorii oprogramowania/pliku/procesu i samodzielnej przydzielenie oprogramowania/pliku/procesu do kategorii.
4.4.7.1. W oparciu o Machine learning system umożliwia analizę procesów oraz przypisanie im odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem uruchamianych procesów.
4.4.7.2. Automatyczne przypisanie kategorii do każdego uruchomionego procesu.
4.4.7.3. Niezależność od zewnętrznych dostawców bazy wzorców procesów.
4.4.8. System zbiera szczegółowe informacje o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji).
4.4.9. System umożliwia odczytywanie identyfikatorów i kluczy produktowych dla systemu operacyjnego oraz dowolnego oprogramowania, tam gdzie jest to tylko technicznie możliwe.
4.4.10. System wspiera następujące typy licencji: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value (Company wide), MOLP Open Value (non-Company wide), MOLP Open Value Subscription, CAL, SAAS, Trial, Shareware, Cal Per User.

4.4.11. System automatycznie klasyfikuje i rozlicza licencje OEM dla systemów operacyjnych oraz licencje typu freeware dla aplikacji.
4.4.12. System musi pomijać w rozliczeniu licencje wygasłe (po terminie ważności) i informować administratora o wygasaniu licencji.
4.4.13. System musi umożliwiać wyróżnianie licencji zabezpieczonych kluczami sprzętowymi.
4.4.14. System automatycznie wskazuje liczbę posiadanych licencji oraz liczbę używanego oprogramowania (pokazuje braki oraz nadwyżki).
4.4.15. System automatycznie uwzględnia i rozlicza licencje typu Upgrade i Downgrade wg zdefiniowanych przez użytkownika reguł.
4.4.16. System prezentuje datę instalacji oprogramowania.
4.4.17. System umożliwia ewidencję licencji (data zakupu, cena, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT, nr zapotrzebowania) poprzez rejestrację dokumentów źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium.
4.4.18. System umożliwia przypisanie licencji do użytkownika i/lub komputera oraz udostępnia informację o licencjach zarejestrowanych i jednocześnie wolnych (nieprzypisanych).
4.4.19. System umożliwiać zbieranie informacji na temat uruchamianych aplikacji na inwentaryzowanych komputerach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji). System musi posiadać mechanizm zabezpieczający przed powstaniem niekompletnych lub niewłaściwych zapisów w wyniku braku zasilania lub innych awarii inwentaryzowanego systemu/sprzętu).
4.4.20. System musi udostępniać informację o uruchamianych aplikacjach w okresie 3/6/12 miesięcy oraz udostępniać datę ostatniego uruchomienia.
4.4.21. System musi automatycznie wyliczać przybliżone oszczędności z zakupionych a nie zainstalowanych aplikacji, przybliżone oszczędności z zainstalowanych a niewykorzystanych licencji oraz przybliżone nakłady konieczne na uzyskanie pełnej legalności.
4.4.22. System musi umożliwiać podgląd historii zmian aplikacji i pakietów na komputerach.
4.4.23. System musi umożliwiać zdalne odinstalowanie oprogramowania na jednym bądź wybranych komputerach.
4.4.24. System musi udostępniać informacje o stopniu wykorzystania aplikacji / pakietów dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej.
4.4.25. System musi udostępniać informacje o stopniu wykorzystania oprogramowania typu web dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej.

4.5. Wzorce aplikacji i pakietów

4.5.1. System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 3,5 tys. wzorców aplikacji, 1,3 tys. producentów, 21 tys. plików, 1,5 tys. wbudowanych treści umów licencyjnych różnych producentów oprogramowania.
4.5.2. System musi udostępniać informacje dotyczące plików, na podstawie których zidentyfikowana została dana aplikacja.
4.5.3. System musi prezentować informacje o ilości i dacie publikacji posiadanej bazy wzorców oprogramowania.
4.5.4. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania.
4.5.5. Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów.
4.5.6. System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu.
4.5.7. System musi rozpoznawać wersję i edycję zainstalowanych pakietów Microsoft Office (tam gdzie jest to technicznie możliwe (np. Microsoft Office 2007 Professional, Microsoft Office 2007 Standard, Microsoft Office 2003 Standard itd.).

4.6. Inwentaryzacja sprzętu komputerowego

4.6.1. System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem).
4.6.2. System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language.
4.6.3. System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu).
4.6.4. System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania.
4.6.5. System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza począwszy od wskazanego miejsca w hierarchii kluczy rejestru.
4.6.6. System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).
4.6.7. System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).
4.6.8. System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku.
4.6.9. System musi umożliwiać skanowanie uprawnień użytkowników oraz grup użytkowników wraz z informacją o uprawnieniach, czy konto jest włączone, zablokowane, czy wymagana jest zmiana hasła, czy hasło wygasa, czy hasło jest wymagane).
4.6.10. System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu.
4.6.11. System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent).
4.6.12. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne.
4.6.13. System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.
4.6.14. System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik)
4.6.15. System umożliwia dodawanie notatek do każdej pozycji sprzętu.
4.6.16. System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).
4.6.17. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium.
4.6.18. System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja).

4.7. Inwentaryzacja urządzeń podłączanych do komputera
4.7.1. System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.
4.7.2. System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.
4.7.3. System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika).

4.8. Inwentaryzacja urządzeń innych niż komputery
4.8.1. System musi umożliwiać inwentaryzację manualną (ewidencję) sprzętu innego niż komputery: np. drukarki, switche, routery, monitory, pamięci masowe itp.
4.8.2. System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/porcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać SNMP w wersji 1/2c/3.
4.8.3. Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.
4.8.4. System musi zbierać informacje o jakości połączenia:
4.8.4.1. Czas odpowiedzi serwisów (usług) podawany w milisekundach:
4.8.4.1.1. Średni czas odpowiedzi.

4.8.4.1.2. Minimalny czas odpowiedzi.
4.8.4.1.3. Maksymalny czas odpowiedzi.
4.8.4.2. Ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat.
4.8.5. System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają agenta, a w przypadku, gdy takiego agenta nie posiadają powinien umożliwić zdalną instalację agenta.
4.8.5.1. Posiada niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci
4.8.5.2. Baza wzorców musi zawierać ponad 100 monitorowanych portów i usług.
4.8.6. System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci.
4.8.6.1. System musi umożliwiać generowanie map według dowolnych filtrów użytkownika.
4.8.7. System umożliwia wprowadzanie dowolnych notatek oraz zdarzeń serwisowych.
4.8.8. System musi monitorować zmiany ewidencyjne i ruchy sprzętu.
4.8.9. System musi umożliwiać przypisanie urządzenia do użytkownika, ewidencję napraw, gwarancji.
4.8.10. System musi mieć możliwość przypominania o upływającym terminie gwarancji.
4.8.11. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu.
4.8.12. System udostępnia informację o wartości wprowadzonego sprzętu.
4.8.13. System musi umożliwiać samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów oraz zapewniać automatyczną numerację tych dokumentów zapewniającą unikatowość.
4.8.14. System musi pozwalać na kopiowanie (duplikację) dowolnego urządzenia dowolną ilość razy.
4.8.15. System musi pozwalać na ewidencję umów utrzymaniowych (SLA) w odniesieniu do zaewidencjonowanych licencji oraz urządzeń w zakresie co najmniej: nazwa, okres, data dokumentu, numer dokumentu, dostawca, osoba kontaktowa, wartość, opis, warunki oraz umożliwiać dołączenie dowolnej ilości załączników z repozytorium i powiązanie umowy utrzymaniowej z dowolną ilością zasobów (urządzenia, licencje).

4.9. Zdalna administracja komputerami
4.9.1. System ma automatyczne wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika.
4.9.2. System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro.
4.9.3. System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączanie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji.
4.9.4. System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6).
4.9.5. System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji (service pack, patch).
4.9.6. System umożliwia zdalne podłączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC.
4.9.7. System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie.
4.9.8. System musi umożliwiać uruchomienie sesji Ultra VNC w trybie podłączenia się do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejęcia dostępu).
4.9.9. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania.
4.9.10. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych,

czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego.

4.9.11. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status).

4.9.12. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, windows powershell. System posiada co najmniej 70 predefiniowanych poleceń.

4.9.13. System musi umożliwiać zdalne połączenia do wielu komputerów jednocześnie, podgląd i operowanie na pulpitach tych komputerów w technologii WEBRTC.

4.9.14. System musi umożliwiać za pomocą technologii WEBRTC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalację oprogramowania, poprawek i aktualizacji (service pack, patch).

4.9.15. System musi umożliwiać poprzez technologię WEBRTC zdalne zarządzanie plikami (tworzenie, kopiowanie, usuwanie, przesyłanie) i wykorzystanie wiersza poleceń (cmd) oraz powershell bez konieczności podłączenia do komputera.

4.9.16. System musi umożliwiać nagrywanie sesji połączeń WEBRTC jak i nawiązywanie komunikacji z użytkownikiem podczas sesji (czat).

4.9.17. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.

4.9.18. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.

4.10. Automatyzacja

4.10.1. System ma mieć możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące.

4.10.2. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania danej czynności (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych, a także zatrzymania/uruchomienia harmonogramu uruchomienia dla każdej z czynności.

4.10.3. System musi mieć możliwość definiowania czynności wykonywanych automatycznie.

4.10.4. System musi być wyposażony w następujące mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów).

4.10.5. System musi być wyposażony w mechanizmy informowania - wysyłania komunikatów (alerty) o: zasobach zakazanych (pliki erotyczne i pornograficzne), zasobach multimedialnych (pliki multimedialne), nowych komputerach w bazie danych, braku skanowania komputerów, brakach w licencjach, niewłaściwych datach systemowych komputerów, urządzeniach bez użytkowników, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, wygasaniu serwisu lub licencji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu sieci, nadmiernym obciążeniu sieci na komputerze, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, upływającej gwarancji,

4.10.6. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).

4.10.7. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)

4.10.8. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów.

4.10.9. Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/wtorek/środa/czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień

wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania.

4.10.10. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie.

4.11. Zarządzanie magazynem IT

4.11.1. System musi umożliwiać obsługę magazynu IT.

4.11.2. System musi umożliwiać obsługę dowolnej ilości magazynów w różnych lokalizacjach.

4.11.3. System musi umożliwiać obsługę dokumentów PZ, WZ, MM+, MM-, LI.

4.11.4. System musi prowadzić ewidencję materiałów w magazynach w oparciu o metodę FIFO (pierwsze przyszło pierwsze wyszło).

4.11.5. System musi umożliwiać obsługę kodów kreskowych dla materiałów w magazynach.

4.11.6. System musi udostępniać informację o wartościach materiałów w poszczególnych magazynach, stanach materiałów w magazynach, dokumentach dotyczących danego materiału w dowolnym magazynie.

4.12. Repozytorium

4.12.1. Konsola administracyjna musi być wyposażona w repozytorium dokumentów dowolnego typu.

4.12.2. Repozytorium musi umożliwiać: dodawanie nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów (znaczniki TAG) więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium w dowolnym miejscu systemu, uzyskanie informacji w jakich miejscach systemu dany dokument repozytorium występuje.

4.13. Kody kreskowe

4.13.1. System wspiera obsługę kodów kreskowych jedno i dwuwymiarowych.

4.13.2. System wspiera parametryzację kodu w zakresie wielkości graficznej kodu.

4.13.3. System pozwala w każdym momencie na zmianę typu i atrybutów kodu.

4.13.4. System informuje o błędzie generacji kodu, np. na skutek niewłaściwej długości wprowadzonego ciągu znaków w stosunku do danego standardu kodu.

4.13.5. Istnieje możliwość podglądu kodu oraz jednostkowego i masowego wydruku kodu / kodów.

4.13.6. System musi generować kody kreskowe (jedno i dwuwymiarowe) dla każdego zaewidencjonowanego urządzenia w standardzie wybranym przez użytkownika: aztec, codabar, code128, code39, dataMatrix, EAN128, EAN13, EAN8, interleaved2of5, ITF14, PDF417, POSTNET, qrcode, royalMailCBC, UPCA, UPCE, USPSIntelligentMail.

4.13.7. Obsługa kodów kreskowych nie może wymagać instalacji czcionek.

4.13.8. Parametry kodu kreskowego (wymiary, wielkość i typ czcionki) muszą być definiowalne.

4.13.9. System musi umożliwiać współpracę z zewnętrznymi czytnikami kodów.

4.14. System szkolenia pracowników za pomocą wiadomości.

4.14.1. System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów.

4.14.2. System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa”, „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa”, „Postępowanie w przypadku naruszenia tajemnicy”, „Udostępnienie informacji stanowiących tajemnicę”.

4.14.3. Formatowanie treści musi być zgodne z HTML.

4.14.4. System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych).

4.14.5. System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców.

4.14.6. Użytkownik otrzymujący wiadomość musi być powiadamiany wizualne i dźwiękowo o otrzymaniu nowej wiadomości.

4.14.7. Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.

4.14.8. System musi posiadać zabezpieczenie (np. synchronizowany z serwerem znacznik czasowy) odporne na zmiany czasu na lokalnym komputerze (użytkownika) a pozwalające na jednoznaczne ustalenie daty i godziny dostarczenia i odczytania wiadomości.

4.14.9. System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników.

4.14.10. System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem).

4.14.11. System musi posiadać możliwość eksportu / importu treści.

4.15. Monitorowanie drukarek sieciowych i wydruków
- 4.15.1. System musi posiadać możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa).
- 4.15.2. Ewidencja wydruków musi obejmować: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera z którego dokonano wydruku, format dokumentu, informację i jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor.
- 4.15.3. System dla każdego wydruku, dla każdej drukarki musi obliczać rzeczywisty koszt wydruku w oparciu o wbudowany cennik wydruków obejmujący cenę papieru (w zależności od formatu) oraz cenę materiałów eksploatacyjnych (toner, tusz) dla danej drukarki, typu wydruku, rozmiaru papieru.
- 4.15.4. System musi generować zestawienia pozwalające ustalić miejsca powstawania kosztów wydruków (komórki organizacyjne, użytkownicy) oraz stopień obciążenia poszczególnych urządzeń drukujących.
- 4.15.5. System musi prognozować ilość i koszt wydruków na wszystkich drukarkach w okresie kolejnych 3,6,12 miesięcy.
- 4.15.6. System musi pozwalać na grupowanie (kojarzenie) drukarek wg sterowników.
- 4.15.7. Dla każdej z drukarek SNMP system musi udostępniać informacje: nr seryjny, IP, MAC, bieżący status drukarki, całkowitą ilość wydrukowanych stron, ilość wydrukowanych stron od uruchomienia, błędy, alerty, dostępne porty, stan pokryw, interfejsów sieciowych, rodzaj i ilości pamięci całkowitej i wykorzystanej, informacje o poziomie materiałów eksploatacyjnych

4.16. Monitorowanie stron www
- 4.16.1. System musi posiadać możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej.
- 4.16.2. Ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek.
- 4.16.3. Ewidencja otwieranych stron musi działać również, gdy otwierana jest strona z połączeniem szyfrowanym (https).
- 4.16.4. Ewidencja musi obejmować co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony, łączny czas korzystania, czas aktywności, czas pasywności.
- 4.16.5. W oparciu o algorytmy sztucznej inteligencji - machine learning oraz deep learning system umożliwia analizę treści rtcstron www oraz przypisanie im – w oparciu o treść – odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem odwiedzanych stron.
- 4.16.6. Każda odwiedzona strona otrzymuje atrybuty: czy SSL, czy jest bezpieczna, czy zawiera przekierowania, czy znajduje się na liście CERT, czy znajduje się na liście stron hazardowych, czy kategoria strony jest bezpieczna, czy jest produktywna.

4.17. Monitorowanie dziennika zdarzeń
- 4.17.1. System musi posiadać możliwość monitorowania dziennika zdarzeń wszystkich komputerów.
- 4.17.2. Ewidencja zdarzeń musi następować w oparciu o definiowalną kategorię zdarzenia: critical, error, warning, info, audit failure, audit success, debug oraz typ dziennika: aplikacja, bezpieczeństwo, system.
- 4.17.3. System musi pozwalać na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia.
- 4.17.4. Ewidencja musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia.
- 4.17.5. System musi umożliwiać monitorowanie komunikatów Syslog.

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

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

komputera docelowego, adres portu połączenia.

4.20. Repozytorium CMDB – centralna baza systemu umożliwiająca import i eksport danych zarówno poprzez API jak też za pomocą wbudowanego import/eksporta, na którą składają się:

4.20.1. Active Directory - lista skonfigurowanych z konsolą serwerów LDAP, z których są importowane i aktualizowane dane o użytkownikach. System pozwala na wprowadzanie dowolnej ilości serwerów dla różnych domen.

4.20.2. Kontenery dokumentów - grupy, do których można przypisywać zapisane w systemie dokumenty w celu sortowania.

4.20.3. Kategorie aplikacji - lista kategorii, do których przynależą wykorzystywane przez użytkowników aplikacje.

4.20.4. Budżet - zestawienie typów budżetów (kosztów) zaewidencjonowanych w systemie.

4.20.5. Komputery - lista zinwentaryzowanych komputerów, podzielonych wg typu autoryzacji. Widok rekordu zawiera szczegółowe dane dotyczące danego komputera.

4.20.6. Dokumenty - repozytorium dokumentów zapisanych w systemie.

4.20.7. eLearning - zdefiniowane wiadomości typu eLearning. Wykorzystywane są do wysyłania użytkownikom szkoleń wbudowanych w system, zgodnie ze zdefiniowanym harmonogramem.

4.20.8. Kategorie plików - lista typów plików kategoryzowanych przez system. Administrator ma możliwość zdefiniowania własnych grup, do których pliki będą przydzielane, według wpisanej maski.

4.20.9. Pliki - lista zinwentaryzowanych plików ze wszystkich komputerów.

4.20.10. Licencje - zestawienie licencji zapisanych w bazie systemu, które administrator może przypisywać do poszczególnych użytkowników.

4.20.11. Typy licencji - lista typów licencji.

4.20.12. Lokalizacje - lista zdefiniowanych lokalizacji, do których administrator może przypisać poszczególnych użytkowników. W odróżnieniu od struktury organizacyjnej dane nie są importowane z Active Directory.

4.20.13. Typy urządzeń - lista typów urządzeń.

4.20.14. Urządzenia - lista urządzeń podzielonych wg typu.

4.20.15. Producenci / Dostawcy - lista producentów i dostawców.

4.20.16. Pamięć masowa - zestawienie dysków twardych z komputerów.

4.20.17. Porty sieciowe - lista monitorowanych portów sieciowych.

4.20.18. Usługi sieciowe - lista monitorowanych usług sieciowych.

4.20.19. Udostępnione zasoby sieciowe - lista udostępnionych zasobów sieciowych.

4.20.20. Sieci - lista definiowalnych ręcznie sieci, do których administrator może ręcznie przypisywać komputery.

4.20.21. Systemy operacyjne - zestawienie unikalnych systemów operacyjnych.

4.20.22. Struktura org. - zestawienie struktur organizacyjnych zdefiniowanych bądź importowanych z Active Directory.

4.20.23. Kategorie procesów - lista kategorii, do których będą przypisywane procesy aplikacji uruchamianych przez użytkowników. Klasyfikacja procesów odbywa się za pomocą algorytmów sztucznej inteligencji.

4.20.24. Serwery - lista zinwentaryzowanych serwerów.

4.20.25. Usługi - zestawienie usług działających na komputerach.

4.20.26. Oprogramowanie - lista zinwentaryzowanego i monitorowanego oprogramowania.

4.20.27. Pamięć masowa USB - lista urządzeń pamięci masowej USB.

4.20.28. Administratorzy - lista administratorów systemu,

4.20.29. Użytkownicy / pracownicy - lista pracowników.

Kategorie WWW - lista kategorii stron WWW wykorzystywanych w procesie klasyfikacji stron internetowych. Klasyfikacja oparta o sztuczną inteligencję.

4.21. Worktime manager

4.21.1. System musi być wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników.

4.21.2. Dane muszą być prezentowane w formie interaktywnych widgetów oraz w formie danych analitycznych.

4.21.3. Dane dla grup użytkowników muszą być skumulowane oraz analityczne.

4.21.4. Prezentacja danych odbywa się poprzez wskazanie pracownika lub grupy pracowników oraz wybranie okresu danych źródłowych.

4.21.5. Informacje dotyczące prezentowane w panelu to informacja o otwartych sesjach, informacja

o sesjach historycznych, informacja o czasie zalogowania użytkownika, informacja o czasie pracy komputera, informacja o aktywności użytkownika w aplikacjach, informacja o produktywności użytkownika w aplikacjach, informacja o produktywności, wykorzystywanych aplikacjach, odwiedzonych stronach www z podziałem na kategorie stron, informacja o uruchomionych procesach z podziałem na kategorie, informacja o aktywności na stronach www, informacja o wykonanych wydrukach (nazwa dokumentu, data i godzina wydruku, drukarka, ilość stron, rodzaj wydruku – czarno-biały czy w kolorze, koszt wydruku), informacja o transferze sieciowym, informacja o zależności czasu pracy w trybach: zalogowany/ uśpiony/ wylogowany.

4.21.6. System musi umożliwić wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje powinny być aktualizowane zgodnie z harmonogramem połączenia z domeną.

4.21.7. System musi prezentować w formie tabelarycznej informacje o dokumentach (np. protokoły przekazania i zwrotu sprzętu), komputerach i urządzeniach, które zostały przypisane użytkownikowi.

4.21.8. System musi posiadać widgety prezentujące dane w wybranym przedziale czasu: czas zalogowania – dni, czas pracy komputera – dni, aktywność w aplikacjach, produktywność w aplikacjach, produktywność w czasie pracy, czas pracy w aplikacjach, czas spędzony na stronach www wg kategorii stron, czas spędzony w aplikacjach (procesach) wg kategorii procesu, czas aktywność na stronach www, stron wydruku wg dokumentów, transfer sieciowy, czas pracy wg zalogowany/ wylogowany / uśpiony, czas aktywności w godzinach pracy.

4.22. Raportowanie i eksport danych

4.22.1. Systemu musi umożliwiać wyeksportowania wybranych lub wszystkich danych do formatu xls, csv, OpenOffice calc, html, mht, xml, jpeg, png, gif, bmp.

4.22.2. System musi mieć możliwość kategoryzowania raportów (spośród wszystkich raportów) oraz dodawania raportów użytkownika (zaprojektowanych przez użytkownika).

4.22.3. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów.

4.22.4. Generowanie raportu musi odbywać się po stronie serwera, a nie klienta.

4.22.5. System musi umożliwiać wieloinstancyjność raportowania (wiele otwartych raportów jednocześnie z wielu widoków).

4.22.6. System musi mieć możliwość generowania i wyświetlania dowolnych wieloparametrycznych raportów w standardzie SAP Crystal Reports (rpt).

4.22.7. System musi umożliwiać eksport danych z raportu do formatów: RPT, PDF, XLS, DOC, RTF.

4.22.8. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).

4.22.9. System musi posiadać co najmniej 150 zdefiniowanych raportów dotyczących wszystkich obszarów funkcjonalnych.

4.22.9.1. Raporty z zakresu komputerów

- Komputery – Karta graficzna – Procesor
- Komputery – Serwery wg systemu operacyjnego
- Komputery wg procesora – Skrócony
- Komputery wg procesora – Wszystkie
- Komputery wg producenta – Skrócony
- Komputery wg producenta – Wszyscy
- Komputery wg struktur organizacyjnych – Skrócony
- Komputery wg struktury organizacyjnej – Wszystkie
- Komputery wg systemów operacyjnych – Skrócony
- Komputery wg systemów operacyjnych – Wszystkie
- Komputery wg typu – Desktop
- Komputery wg typu – Hyper-V
- Komputery wg typu – Mobile
- Komputery wg typu – Nieokreślone
- Komputery wg typu – Server
- Komputery wg typu – Virtual Machine
- Komputery wg typu – VMWare
- Komputery wg typu – Wszystkie typy

- Zestawienie komputerów wg typu – Skrócony
- Komputery online
- Komputery niezautoryzowane
- Komputery offline
- Komputery online
- Komputery w magazynie
- Komputery w naprawie
- Komputery wszystkie
- Komputery wycofane
- Komputery zablokowane
- Komputery zautoryzowane
- Komputery zlikwidowane
- Komputery z Intel Anti-Theft
- Komputery z Intel VPro

4.22.9.2. Raporty z zakresu urządzeń

- Urządzenia – Notatki
- Urządzenia – USB – Dodane
- Urządzenia – USB – Wykryte
- Urządzenia – USB – Wszystkie
- Urządzenia – USB – Biała lista
- Urządzenia – Serwis
- Urządzenia – Inwentaryzacja – Kody kreskowe
- Urządzenia – Inwentaryzacja
- Urządzenia – Inwentaryzacja – Porównanie inwentaryzacji
- Urządzenia – Utrzymanie
- Urządzenia

4.22.9.3. Raporty z zakresu sieci

- Sieć – Wykryte
- Sieć – Historia
- Sieć – Ostanie skanowanie

4.22.9.4. Raporty z zakresu oprogramowania

- Oprogramowanie – Systemy operacyjne – Wszystkie
- Oprogramowanie – Systemy operacyjne – Instalacje OEM
- Oprogramowanie – Systemy operacyjne – Szczegóły
- Oprogramowanie – Systemy operacyjne – Historia audytów
- Oprogramowanie – Aplikacje – Wszystkie
- Oprogramowanie – Aplikacje – Monitorowane
- Oprogramowanie – Aplikacje – Szczegóły
- Oprogramowanie – Aplikacje – Historia audytów
- Oprogramowanie – Pakiety – Wszystkie
- Oprogramowanie – Pakiety – Szczegóły
- Oprogramowanie – Pakiety – Historia audytów
- Oprogramowanie – Bazy danych – Wszystkie
- Oprogramowanie – Bazy danych – Express
- Oprogramowanie – Bazy danych – Pozostałe
- Oprogramowanie – Bazy danych – per Core
- Oprogramowanie – Rejestry – Razem
- Oprogramowanie – Rejestry – Szczegóły
- Oprogramowanie – Rejestry – Ostatnio zainstalowane
- Oprogramowanie – Klucze produktu
- Oprogramowanie – Wykorzystanie – Użycie – Wszystkie
- Oprogramowanie – Wykorzystanie – Oszczędności
- Oprogramowanie – Wykorzystanie – CAL
- Oprogramowanie – Wykorzystanie – CAL WEB
- Oprogramowanie – Monitorowanie – Uruchomienia

- Oprogramowanie – Monitorowanie – Aktywność ogółem

4.22.9.5. Raporty z zakresu osób

- Osoby – Protokół standardowy
- Osoby – Protokół rozszerzony

4.22.9.6. Raporty z zakresu plików i multimediów

- Pliki i multimedia – Archiwa
- Pliki i multimedia – Audio
- Pliki i multimedia – Erotyka
- Pliki i multimedia – Grafika
- Pliki i multimedia – Wideo
- Pliki i multimedia – Wykonywalne
- Pliki i multimedia – Zmiany plików

4.22.9.7. Raporty z zakresu magazynu

- Magazyn – Dokumenty
- Magazyn – Stany
- Magazyn – Materiały
- Magazyn

4.22.9.8. Raporty z zakresu finansów

- Finanse – Urządzenia
- Finanse – Licencje
- Finanse – Wydruki wg drukarki
- Finanse – Wydruki wg sterownika
- Finanse – Wydruki użytkownicy
- Finanse – Magazyn

4.22.9.9. Raporty z zakresu serwera wiadomości

- Serwer wiadomości – Komunikator – Historia
- Wiadomość cykliczna – wg wiadomości
- Serwer wiadomości – Komunikator – Rozmowy
- Serwer wiadomości – Wiadomości wysłane – wg komputera
- Serwer wiadomości – Wiadomości wysłane – wg odbiorcy
- Serwer wiadomości – Wiadomości wysłane – wg wiadomości
- Serwer wiadomości – Wiadomości wysłane – wg wysyłającego
- Serwer wiadomości – Wiadomości – Aktywne cykle

4.22.9.10. Raporty z zakresu serwera monitorującego

- Serwer monitorujący – Logowanie agentów
- Serwer monitorujący – eServer
- Serwer monitorujący – Alerty systemowe
- Serwer monitorujący – Historia logowań
- Serwer monitorujący – Dzienniki zdarzeń – Powiadomienia systemowe
- Serwer monitorujący – Dzienniki zdarzeń – Dzienniki
- Serwer monitorujący – Dzienniki zdarzeń – Sesje RDP
- Serwer monitorujący – Transfer sieciowy – Procesy
- Serwer monitorujący – Drukowanie
- Serwer monitorujący – Drukowanie – Razem
- Serwer monitorujący – Drukowanie – Razem SNMP
- Serwer monitorujący – Drukowanie – Prognoza
- Serwer monitorujący – Usługi – Wszystkie
- Serwer monitorujący – Usługi – Szczegóły
- Serwer monitorujący – Harmonogram zadań
- Serwer monitorujący – Sesje VNC
- Serwer monitorujący – Intel AMT
- Serwer monitorujący – Strony www – Odwiedzone
- Serwer monitorujący – Strony www – Aktywność ogółem
- Serwer monitorujący – USB
- Serwer monitorujący – Wydajność – CPU

- Serwer monitorujący – Wydajność – Dysk
- Serwer monitorujący – Wydajność – Dysk (razem)
- Serwer monitorujący – Wydajność – Pamięć
- Serwer monitorujący – Wydajność – Procesy
- Serwer monitorujący – Wydajność – Sieć

4.22.9.11. Raporty z zakresu serwera zadań

- Serwer zadań – Logi
- Serwer zadań – Zadania cykliczne

4.22.9.12. Raporty z zakresu serwera automatyzacji

- Serwer automatyzacji – Automaty
- Serwer automatyzacji – Logi

4.22.9.13. Raporty z zakresu raportów

- Raporty – Harmonogram
- Raporty – Harmonogram – Historia

4.22.9.14. Raporty z zakresu repozytorium

- Repozytorium – Dokumenty
- Repozytorium – e-Learning
- Repozytorium – Kategorie aplikacji
- Repozytorium – Kategorie plików
- Repozytorium – Kategorie procesów
- Repozytorium – Kategorie www
- Repozytorium – Producenci Dostawcy
- Repozytorium – Typy licencji
- Repozytorium – Zdalna instalacja – Repozytorium
- Repozytorium – Zdalna instalacja – Logi

4.22.9.15. Raporty z zakresu ustawień

- Ustawienia – Administratorzy – Wszystkie
- Ustawienia – Dane firmy
- Ustawienia – Struktura organizacyjna
- Ustawienia – Budżet
- Ustawienia – Sieci

4.22.10. System musi posiadać możliwość ustalenia harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu.

4.22.10.1. Wynikiem wykonania harmonogramu jest raport w formacie pdf.

4.22.10.2. Harmonogram można skonfigurować.

4.23. Powiadomienia

4.23.1. System musi umożliwiać generowanie powiadomienia w formie alertu w konsoli systemu, wiadomości email wysłanej na wybrane adresy oraz wiadomości SMS na wskazane numery telefonów.

4.23.2. System musi umożliwiać tworzenie wybranych powiadomień wiele razy z określeniem innych grup obiorców

4.23.3. System musi umożliwiać edycję treści wysyłanych powiadomień i możliwość korzystania z danych umieszczonych w systemie w treści powiadomienia.

4.23.4. System musi posiadać co najmniej 30 zdefiniowanych powiadomień dotyczących obszarów funkcjonalnych

4.23.5. Powiadomienia z zakresu oprogramowania

- Odinstalowano oprogramowanie
- Wykryto niezgodność ze schematem oprogramowania
- Wykryto nowe oprogramowanie

4.23.6. Powiadomienia z zakresu sieci

- Monitorowana usługa sieciowa przestała odpowiadać
- Monitorowane urządzenia z problemami
- Monitorowane urządzenie jest offline
- Problem ze stroną WWW
- Serwis WWW nie odpowiada
- Serwis WWW odpowiada niewłaściwym komunikatem

- Średni czas odpowiedzi usługi przekroczył wartość X ms
- Transfer sieciowy na komputerze przekroczył X MB / Y min
- W sieci pojawiły się duplikaty adresów IP
- W sieci pojawiły się duplikaty adresów MAC
- Wykryto dużą ilość danych wysyłanych przez dany port w switch'u
- Wykryto nowe urządzenie
- Wykryto urządzenie z odblokowanym portem X
- Wykryto urządzenie z usługą X
- Wykryto zmianę adres IP komputera
- Wykryto zmianę statusów portów w switch'u

4.23.7. Powiadomienia z zakresu sprzętu

- Interfejs sieciowy wyłączony
- Parametr lub parametry S.M.A.R.T. przekroczyły dozwolone wartości
- Podłączono urządzenie USB
- Wykryto zmianę w sprzęcie (WMI)

4.23.8. Powiadomienia z zakresu systemu

- Mało miejsca na dysku C
- Pojawił się błąd w dzienniku zdarzeń Windows
- Wykryto problem z usługą systemu Windows
- Wykryto zmianę nazwy komputera
- Wysokie użycie pamięci RAM
- Zmieniono informację o systemie

4.23.9. Powiadomienia z zakresu użytkownika

- Użytkownik odwiedził stronę WWW z wybranej kategorii
- Użytkownik przekroczył limit wydrukowanych stron
- Użytkownik przekroczył transfer sieciowy X MB / Y min

5. Bezpieczeństwo

5.1. System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.

5.2. Uwierzytelnianie do systemu musi być realizowane:

5.2.1. z wykorzystaniem imiennego konta użytkownika i hasła,

5.2.2. z wykorzystaniem imiennego konta administratorów aplikacji i hasła,

5.2.3. za pośrednictwem jednokrotnego uwierzytelniania poprzez Active Directory,

5.2.4. za pośrednictwem jednokrotnego uwierzytelniania poprzez CAS,

5.2.5. za pomocą kluczy uwierzytelniających.

5.2.6. za pomocą kodu na maila

5.3. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej.

5.4. Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków).

5.5. Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport.

5.6. System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie.

5.7. Uwierzytelnianie za pomocą kluczy

5.7.1. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkownikom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP.

5.7.2. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 512/1024/RSA 2048 bit, ECDSA 192/256 bit, DES/3DES, AES 128/192/256 bit, SHA-1 / SHA-256.

5.7.3. Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 7/8.1/10 i Windows Server 2012/2016/2019.

5.8. System musi udostępniać historię korzystania z poszczególnych opcji przez wybranych użytkowników/administratorów.

5.9. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy agentami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera.

5.10. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nieprzyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.
5.11. System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych.
5.12. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy).
5.13. System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od agentów.
5.14. System musi zapewniać:
5.14.1. Pełne logowanie błędów w celu weryfikowania nieprawidłowości.
5.14.2. Przechowywanie logów systemowych.
5.14.3. Przechowywanie logów bezpieczeństwa.
5.14.4. Przechowywanie logów aktywności użytkowników i administratorów.
5.14.5. Pobieranie logów z agentów z poziomu konsoli administracyjnej.
5.14.6. Możliwość eksportu logów.
5.14.7. Definiowanie maksymalnego czasu przechowywania plików log.
5.15. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.
6. Wsparcie, pomoc, informacje dodatkowe
6.1. System musi posiadać dokumentację w postaci min. 20 filmów instruktażowych/nagrań z webinarów w języku polskim.
6.2. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim.
6.3. Pomoc techniczna musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.
6.4. Zdalne wykonanie instalacji, konfiguracji i profilowanie systemu.
6.5. Minimum 2 godziny szkolenia z obsługi dostarczonego systemu.
6.6. Certyfikat dla administratorów przeszkolonych z użytkowania systemu.

6.11. Instalacja, konfiguracja, wdrożenie, utrzymanie. – szt. 1 – wymagania minimalne

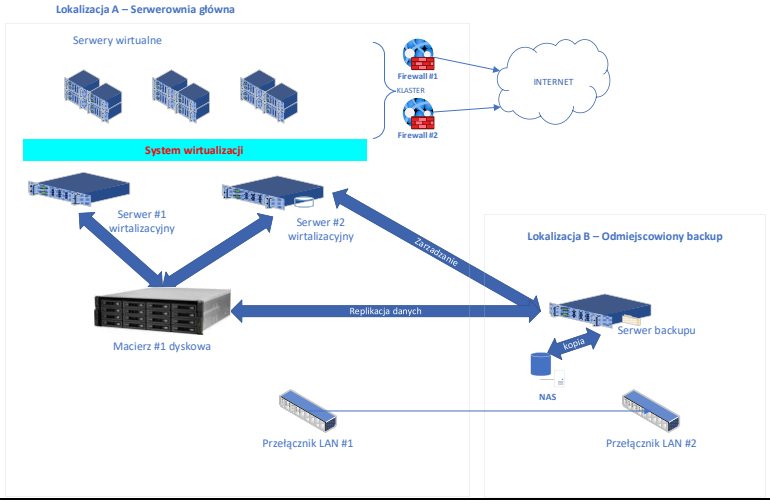
Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.		
1.	**Usługi**	Celem prac jest przygotowanie środowiska teleinformatycznego, na potrzeby realizacji elementów cyberbezpieczeństwa, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie. Część sprzętowa powinna zostać oparta na systemie wirtualizacji zasobów IT. Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa i wymagań Zamawiającego. Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia. **W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową**. Zamawiający wymaga następującego zakresu usług realizowanego w porozumieniu z Zamawiającym: a) Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia. b) Sporządzenia Dokumentacji Systemu według której nastąpi realizacja.

		Dokumentacja Systemu musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia. W szczególności: i. koncepcję techniczną projektu, która powinna zawierać opis mechanizmów działania systemu z wykorzystaniem dostarczonych i rozbudowywanych elementów sprzętowych. ii. schematy połączeń iii. mechanizmy działania głównych elementów sprzętowych: • sieć LAN - przełączniki sieciowe • klaster wirtualizacyjny • system backupu i archiwizacji danych • system serwerowy • system macierzowy • firewall/UTM iv. iii. mechanizmy działania głównych elementów programowych: • system EDR • system NAC • system domenowy/wirtualizacyjny • system backupu • system zarządzania siecią v. testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności vi. sposób odbioru uzgodniony z Zamawiającym vii. listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu viii. opis przypadków, w których projekt dopuszcza niedziałanie systemu ix. realizacja wdrożenia nastąpi według Planu Wdrożenia po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Planem Wdrożenia.
2.	**Montaż i fizyczne uruchomienie systemu**	**Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:** 1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji. 2. Rozbudowa istniejących zasobów sprzętowych. 3. Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego. 4. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń. 5. Podłączenie całości rozwiązania do infrastruktury Zamawiającego. 6. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu. 7. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów. 8. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym). 9. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające). 10. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ miedzy innymi celem: a. Stworzenia połączeń sieci LAN pomiędzy przełącznikami. b. Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN.

		c. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1. d. Połączenia musza wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.
3.	**Instalacja i konfiguracja oprogramowania**	1. Instalacja i konfiguracja dostarczonego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji. 2. Instalacja i konfiguracja oprogramowania do systemu wykonywania backupu i archiwizacji danych działającego na serwerze backupu. 3. Instalacja dostarczonego oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Zamawiającego). 4. Instalacja i konfiguracja dostarczonych systemów operacyjnych dla serwerów wirtualnych. 5. Instalacja i konfiguracja oprogramowania EDR. 6. Instalacja i konfiguracja oprogramowania NAC. 7. Aktualizacja systemu zarzadzania siecią.
4.	**Konfiguracja przełączników/ sieci LAN:**	Zamawiający wymaga stworzenia połączeń sieciowych pomiędzy wszystkimi lokalizacjami występującymi w projekcie według topologii gwiazdy. Centralnym punktem będzie serwerownia zlokalizowana w Urzędzie. Dostarczone przełączniki urządzaniami będą stanowiły centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI – L2 (warstwa łącza danych) oraz zapewnią wsparcie dla protokołu STP (protokół drzewa rozpinającego). Konfiguracja przełączników w zakresie: a. Przeprowadzenie audytu obecnej topologii oraz konfiguracji. b. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. c. Stworzenia odpowiednich konfiguracji STACK z wykorzystaniem dedykowanych modułów. d. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym). e. Wymagane jest wydzielenie i skonfigurowanie co najmniej stref: • SERWERY • UŻYTKOWNICY WEWNĘTRZNI • UŻYTKOWNICY ZEWNĘTRZNI • MANAGEMENT f. Jeśli jest to konieczne – Zamawiający oczekuje rekonfiguracji adresacji IP w danych strefach (readresacja urządzeń, serwerów, komputerów leży po stronie Wykonawcy) g. Zamawiający wymaga skonfigurowania polityk ruchu pomiędzy strefami na urządzeniach firewall. h. Konfiguracja połączeń pomiędzy przełącznikami sieci LAN. i. Rozpięcie połączeń przełączników IDF na centralne przełączniki CORE z zachowaniem nadmiarowości z wykorzystaniem wszystkich dostępnych portów uplink. ii. Z wykorzystaniem połączeń światłowodowych oraz miedzianych. iii. Agregacja połączeń celem uzyskania pasma nx10Gbps w obu kierunkach ruchu. iv. Należy wykorzystać wkładki o najwyższej możliwej przepustowości dla danego połączenia np.: dla portu o możliwej przepustowości 1/10Gbs (wkładka: SFP/SFP+), należy wykorzystać wkładki SFP+ o przepustowości

		10Gbps. i. Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN. j. Konfiguracja routingu pomiędzy sieciami VLAN na centralnym urządzeniu firewall - klaster; k. Zamawiający wymaga aby wszystkie sieci VLAN (L2) zostały rozpięte na warstwie L2 na urządzeniu firewall – (połączenie TRUNK). l. Zamawiający wymaga skonfigurowania mechanizmów bezpieczeństwa na dostarczonych przełącznikach LAN co najmniej w zakresie: • Konfiguracja mechanizmów DHCP Snooping • Konfiguracja mechanizmów Dynamic ARP Inspection • Konfiguracja mechanizmów Port Security na wskazanych portach przełączników • Konfiguracja mechanizmów 802.1x na wskazanych portach przełączników w oparciu o certyfikaty komputerów (konfiguracja Centrum Certyfikacji oraz polityk leży po stronie Wykonawcy) z wykorzystaniem dostarczonego oprogramowania NAC. m. Ustawienie serwera czasu dla urządzeń sieci LAN – przełączników sieciowych - na klaster firewall. n. Zamawiający wymaga instalacji i konfiguracji serwera logów dla urządzeń sieci LAN (maszyna wirtualna) – przełączników sieciowych, z graficznym interfejsem przeszukiwania. Zamawiający dopuszcza rozwiązania Open Source. o. Zamawiający wymaga instalacji i konfiguracji dedykowanego serwera monitorowania pracy urządzeń sieciowych z graficznym interfejsem przeszukiwania (maszyna wirtualna): przełączniki sieciowe, drukarki, UTM. Zamawiający dopuszcza rozwiązania Open Source. p. Wykonawcza skonfiguruje urządzenia aby raportowały, przesyłały dane do zainstalowanego serwera logów i monitorowania sieci. q. Testowanie obsługi ruchu sieciowego. r. Testowanie skuteczności zabezpieczeń.
5.	**Konfiguracja elementów bezpieczeństwa sieciowego.**	1. Zastawienia klastra HA z istniejącym urządzeniem firewall firmy Fortinet FG-61F. 2. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. 3. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta. 4. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email) 5. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu. 6. Konfiguracja dostarczonych systemów Firewall: a. Konfiguracja podstawowych parametrów b. Konfiguracja translacji adresów NAT c. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, macierze, itp. d. Konfiguracja inspekcji określonych protokołów sieciowych; e. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall; f. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym; g. Testowanie działania bramy 7. Konfiguracja modułów należących do systemu wykrywania włamań IPS: a. Konfiguracja podstawowych parametrów b. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań; c. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego; d. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;

		e. Testowanie działania ochrony IPS 8. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL. a. Przypisanie adresu IP do zarządzania. b. Konfiguracja inspekcji protokołów HTTP, HTTPS; SMTP, FTP, POP3 c. Definicja reguł filtrowania/blokowania d. Integracja z systemem domenowym w celu weryfikacji nawiązywania połączenia poprzez nazwę użytkownika z domeny. 9. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej. 10. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia. 11. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN. 12. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC 13. W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności: a. kontrola dostępu - zapora ogniowa klasy Stateful Inspection b. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar c. ochrona przed atakami - Intrusion Prevention System [IPS/IDS] d. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM. e. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) f. kontrola pasma oraz ruchu [QoS, Traffic shaping] g. Kontrola aplikacji oraz rozpoznawanie ruchu P2P h. Ochrona przed wyciekiem poufnej informacji (DLP) i. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL) j. Inspekcja ruchu SSL k. Ochrony przez atakami na stacje klienckie l. Kontrola pasma 14. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi. 15. Konfiguracja logowania i raportowania. 16. Podłączenie klastra firewall do dostarczonego centralnego sytemu logów.
6.	**Serwery pod wirtualizację**	Zamawiający wymaga instalacji i konfiguracji dostarczonych serwerów celem stworzenia bazy sprzętowej dla klastra niezawodnościowego i wydajnościowego stworzonego na bazie dostarczonych serwerów i oprogramowania do wirtualizacji.
7.	**Serwer backupu**	W ramach projektu przewiduje się wykorzystanie urządzenia - serwera na backupu - miejsce przechowywanie backupu. Na serwerze należy zainstalować oprogramowanie do wirtualizacji – zarządzane z jednego centralnego miejsca, tego samego jak dla serwerów wirtualizacyjnych. System musi zostać podłączony do macierzy produkcyjnej, musie posiadać lokalne repozytoria danych na przestrzeni dyskowej, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na połowie zasobu dyskowego. Natomiast druga część zasobu musi zostać wykorzystana do wykonywania replikacji on-line maszyn wirtualnych na lokalna platformę wirtualizacyjną – na serwerze backupu. Takie podejście ma gwarantować zabezpieczenie kluczowych węzłów sieciowych (serwerów wirtualnych) na dwa sposoby tj. plik off-line maszyny wirtualnej oraz kopia on-line replikowania asynchronicznie według harmonogramu. Wykonywanie backupu musi być powiązane z procedurą sprawdzania poprawności

		jego wykonania oraz automatycznym raportowaniem do jednostki administracyjnej. Mechanizm podłączenia 1. Konfiguracja i podłączenie serwera backupu do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy. 2. Konfiguracja i podłączenie serwera backupu do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN. 3. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q. Logiczny schemat rozbudowywanego systemu backup – stan docelowy. 
8.	**Macierz dyskowa**	Macierz musi być wykorzystywana do gromadzenia i przechowywania „danych produkcyjnych” – wykorzystywanych przez oprogramowanie dziedzinowe. Musi zostać podłączona do środowiska wirtualizacyjnego (klaster serwerów). Ilość i wielkość udziałów dyskowych udostępnionych dla serwerów np.: wirtualizacyjnych zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej.
9.	**Migracja danych**	Dotyczy przeniesienia obecnie wykorzystywanych i rozbudowywanych systemów informatycznych na nowe dostarczone rozwiązanie sprzętowe z wykorzystaniem wirtualizacji zasobów. Dane (systemy dziedzinowe) musza zostać przeniesione na nowe zasoby serwerowo-macierzowe. Zakres migracji zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej. Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzinowych.
10.	**Serwer SMTP**	Zamawiający wymaga zainstalowania oraz uruchomienia i skonfigurowania dedykowanego serwera SMTP. Serwer SMTP powinien być uruchomiony na dedykowanym wirtualnym serwerze pracującym pod kontrolą systemu Linux. Serwer SMTP będzie wykorzystywany na potrzeby wysyłania powiadomień systemowych między innymi z: • Urządzeń sieciowych

		• Serwerów • Macierzy dyskowej • Systemu zarządzania kopiami zapasowymi • Systemu wirtualizacji serwerów • Aplikacji Zamawiający wymaga zabezpieczenia serwera w taki sposób, aby uniemożliwić przesyłanie wiadomości z nieautoryzowanych źródeł. Zamawiający wymaga, aby wysyłane powiadomienia były poprawnie dostarczane na zewnętrzne konta email.
11.	**Instalacja i konfiguracja serwera kopii zapasowych konfiguracji urządzeń sieciowych.**	1. Zamawiający wymaga, aby wraz z uruchomieniem dostarczanych urządzeń sieciowych uruchomić serwer – repozytorium konfiguracji z dostarczanych urządzeń np.; przełączników sieciowych oraz innych urządzeń wspierających wykonywanie kopii zapasowych konfiguracji na zasób sieciowy. 2. Serwer musi być uruchomiony na dedykowanej maszynie (dopuszcza się maszynę wirtualną uruchomioną na infrastrukturze wirtualizującej Zamawiającego). 3. Serwer może działać w oparciu o dowolny system operacyjny, Zamawiający powinien uwzględnić cenę licencji w ofercie i dostarczyć ją we własnym zakresie. 4. Serwer może działać w oparciu o dowolne oprogramowanie bądź rozwiązanie autorskie Wykonawcy. Jeżeli takowa jest potrzebna, Zamawiający wymaga dostarczenia licencji. Cena licencji powinna być wliczona w cenę oferty.
12.	**Uruchomienie środowiska wirtualizacyjnego.**	Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w zakresie: 1. Aktywacja licencji oprogramowania wirtualizacyjnego na stronie producenta. 2. Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 3. Przygotowanie macierzy do podłączenia do systemu wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta. 4. Instalacja oprogramowania wirtualizacyjnego na dostarczonych serwerach. 5. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów. 6. Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy. 7. Konfiguracja i podłączenie serwerów wirtualizacyjnych do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN. 8. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q. 9. Przygotowanie koncepcji wirtualizacji fizycznych maszyn. 10. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym. 11. Konfiguracja klastra wysokiej dostępności: a. Konfiguracja mechanizmów HA – w przypadku awarii węzła klastra wirtualne maszyny, które są na nim uruchomione muszą zostać przeniesione na sprawny węzeł klastra bez ingerencji użytkownika. b. Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych

		maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn. c. Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera. 12. Weryfikacja działania klastra wysokiej dostępności. 13. Migracja istniejącej infrastruktury do środowiska wirtualnego. 14. Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową 15. Konfiguracja powiadomień o krytycznych zdarzeniach (email).
13.	**System backupu**	1. Instalacja i rekonfiguracja oprogramowania zarządzającego wykonywaniem kopii zapasowych na dostarczonym serwerze. 2. Aktywacja oraz instalacja niezbędnych licencji. 3. Konfiguracja stacji zarządzającej. 4. Dołączenie klientów do system backupu. 5. Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania: a. kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące; b. kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy; c. kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu; d. kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową; e. musi istnieć możliwość odtworzenia: i. całej wirtualnej maszyny; ii. dysku wirtualnej maszyny; iii. pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa); 6. Zdefiniowanie powiadomień o przebiegu zadania (Zamawiający wymaga skonfigurowania powiadomień na wskazany adres email zawierających, co najmniej: a. Nazwę zadania backupu b. Status zakończenia zadania backupu /Powodzenie, niepowodzenie/ c. Długość trwania zadania backupu d. Ilość zapisanych na taśmie danych 7. Zdefiniowanie powiadomień na wskazany adres email o zdarzeniach: a. Błąd urządzenia b. Uszkodzenie wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi c. Brak miejsca w wewnętrznej bazie danych systemu zarządzania kopiami zapasowymi d. Konieczność przeprowadzenia oczyszczania wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi e. Zdarzenia dotyczące licencji f. Zapełnienia mail-slotu 8. Uruchomienie testowych zadań backupu 9. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email 10. Uruchomienie testowych zadań odtworzenia danych 11. Miejscem przechowywania kopii zapasowych jest: a. serwer backupu. b. NAS 12. na etapie wdrożenia należy ustalić czasy RPO (okresu czasu przez jaki dane mogą być utracone w wyniku awarii) i RTO (okresu czasu w ciągu którego system, który uległ awarii powinien zostać przewrócony) z Zamawiającym

		13. System musi zostać podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na serwerze backupu.
14.	**System EDR**	Zamawiający wymaga podniesienia wersji aktualnie posiadanego oprogramowania antywirusowego do wersji posiadającej moduł XDR. System należy skonfigurować według zaproponowanych wytycznych przez Wykonawcę z uwzględnieniem wymagań Urzędu. Zakres konfiguracji musi zostać zaakceptowany i ustalony z administratorem. Po przeprowadzanej aktualizacji wymagane jest przeszkolenie administratora z całości systemu ze szczególnym uwzględnieniem nowych funkcjonalności.
15.	**System NAC**	System należy skonfigurować według zaproponowanych wytycznych przez Wykonawcę z uwzględnieniem wymagań Urzędu. Zakres konfiguracji musi zostać zaakceptowany i ustalony z administratorem. Po przeprowadzanej instalacji wymagane jest przeszkolenie administratora z całości systemu.
16.	**Oprogramowanie do zarzadzania siecią.**	System należy skonfigurować według zaproponowanych wytycznych przez Wykonawcę z uwzględnieniem wymagań Urzędu. Zakres konfiguracji musi zostać zaakceptowany i ustalony z administratorem. Po przeprowadzanej instalacji wymagane jest przeszkolenie administratora z całości systemu.
17.	**Usługa katalogowa.**	**Instalacja, aktualizacja usługi katalogowej wraz z dodatkowymi komponentami w taki sposób, aby spełnione były poniższe wymagania celem świadczenia e-usług publicznych:**
17.1	**Zaplanowanie liczby serwerów na potrzeby usługi katalogowej oraz serwerów plików**	Taka liczba serwerów, aby w przypadku awarii pojedynczego serwera był zapewniony ciągły dostęp do usługi katalogowej, a w szczególności mechanizmy uwierzytelniania oraz rozwiązywania nazw oraz serwera plików. Zamawiający dopuszcza wykorzystanie serwerów wirtualnych uruchomionych na dostarczonym środowisku wirtualizacyjnym.
17.2	**Wersja systemu operacyjnego serwerów**	Zastosowany system operacyjny musi zapewniać, co najmniej: a) możliwość uruchomienia usługi katalogowej w trybie usługi b) możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń c) możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem (w tym przynależność do grup zabezpieczeń) d) możliwość zarządzania usługą katalogową poprzez interfejs graficzny oraz CLI e) możliwość zainstalowania lokalnego Centrum Certyfikacji zapewniającego wydawanie niekwalifikowanych certyfikatów X.509 umożliwiających uwierzytelnianie na stacjach roboczych i serwerach z wykorzystaniem kart kryptograficznych, szyfrowanie danych
17.3	**Instalacja systemu operacyjnego serwerów**	Instalacja systemu operacyjnego serwerów w taki sposób, aby w łatwy sposób możliwe było włączenie funkcji szyfrowania partycji systemowej za pomocą wbudowanych w system operacyjny mechanizmów. Po instalacji systemy operacyjne muszą zostać prawidłowo aktywowane. Następnie należy zainstalować niezbędne aktualizacje oraz poprawki związane z bezpieczeństwem udostępnione przez producenta systemu operacyjnego.
17.4	**Uruchomienie usługi katalogowej oraz niezbędnych**	Uruchomienie usługi katalogowej, komponentów odpowiedzialnych za rozwiązywanie nazw. Usługa katalogowa musi być uruchomiona na wszystkich serwerach przewidzianych do rozbudowy. Na wszystkich serwerach muszą być uruchomione także komponenty odpowiedzialne za rozwiązywanie nazw. Należy szczególną uwagę zwrócić na poprawne funkcjonowanie mechanizmów replikacji.

	komponentów, migracja danych do/z obecnej usługi katalogowej	Usługę katalogową należy skonfigurować w taki sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowane systemy operacyjne, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem. Utworzenie struktury jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego. Zamawiający wymaga skonfigurowania delegacji uprawnień do zadanych jednostek organizacyjnych dla administratorów niższego poziomu. Administratorzy niższego poziomu powinni mieć uprawnienia do: a) Resetowania haseł użytkowników b) Odblokowywania kont użytkowników c) Zmiany atrybutów „Display Name” oraz „Last name” Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi: a) Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości b) Śledzenie zmian dotyczących tworzenia, usuwania obiektów Zamawiający wymaga skonfigurowania dwóch stacji zarządzających. Zarządzanie środowiskiem będzie się odbywać z poziomu stacji zarządzających (usługa katalogowa, wszystkie możliwe do zarządzania z poziomu stacji zarządzającej komponenty serwerów).
17.	**Konfiguracja polityki haseł oraz polityki blokowania kont**	Konfiguracja globalnej polityki haseł dla domeny: a) Hasło musi zawierać minimum 8 znaków b) Maksymalny czas ważności hasła: do ustalenia z Zamawiającym c) Minimalny czas, po którym możliwa jest zmiana hasła: do ustalenia z Zamawiającym d) Hasło musi spełniać zasady złożoności Konfiguracja polityki haseł dla kadry zarządzającej: a) Hasło musi zawierać minimum 10 znaków b) Maksymalny czas ważności hasła: 30 dni c) Minimalny czas, po którym możliwa jest zmiana hasła: 240 dni d) Hasło musi spełniać zasady złożoności Po 3 nieudanych próbach uwierzytelniania konto powinno być blokowane na 30 minut. Automatyczne anulowanie blokady ma następować po 480 minutach. Szczegółowe dane zostaną przekazane na etapie konfiguracji.
17.	**Stworzenie skryptów służących do tworzenia struktury usługi katalogowej**	Po oddaniu wdrożonego systemu do eksploatacji konieczne będzie tworzenie nowych kont użytkowników, grup zabezpieczeń oraz jednostek organizacyjnych. Zamawiający oczekuje stworzenia przez Wykonawcę skryptów ułatwiających te zadania. **Założenia skryptu tworzącego nowe jednostki organizacyjne oraz grupy:** 1. Możliwość skonfigurowania za pomocą zmiennych w skrypcie, co najmniej: a) ścieżki i nazwy pliku wejściowego b) ścieżki i nazwy pliku logującego c) ścieżki i nazwy pliku wyjściowego (właściwego skryptu) d) nazwy FQDN domeny e) nazwy NetBIOS domeny f) nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty g) ścieżek do udziałów dyskowych SHARE1 oraz SHARE2

2. Skrypt ma pobierać z pliku wejściowego listę jednostek organizacyjnych
3. Skrypt tworzy nowe jednostki organizacyjne w jednostce organizacyjnej nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu
4. Skrypt tworzy nowe grupy zabezpieczeń o nazwie G_Nazwa_Jednoski_Organizacyjnej
5. Skrypt tworzy foldery:
    a) \\DOMENA\Public\SHARE1
    b) \\DOMENA\Public\SHARE2

Foldery muszą posiadać tak ustawione parametry zabezpieczeń, aby użytkownicy nie mogli samodzielnie tworzyć nowych katalogów ani plików w lokalizacjach \\DOMENA\SHARE1 oraz \\DOMENA\SHARE2.

6. Skrypt tworzy podkatalogi: \\DOMENA\Public\SHARE1\Nazwa_Jednostki_Organizacyjnej oraz \\DOMENA\Public\SHARE2\Nazwa_Jednostki_Organizacyjnej
7. Skrypt nadaje uprawnienia do utworzonych podkatalogów według założeń:
    a) \\DOMENA\Public\SHARE1\Nazwa_Jednostki_Organizacyjnej:
        i. Administratorzy Domeny – Pełna kontrola
        ii. Grupa G_Nazwa_Jednostki_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa_Jednostki_Organizacyjnej
        iii. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu
        iv. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze
    a) \\DOMENA\Public\Share2\Nazwa_Jednostki_Organizacyjnej:
        v. Administratorzy Domeny – Pełna kontrola
        vi. Grupa G_Nazwa_Jednostki_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa_Jednostki_Organizacyjnej
        vii. Użytkownicy Uwierzytelnieni - Odczyt
        viii. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu
        ix. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze
8. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina)
9. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania

Założenia skryptu tworzącego nowe konta użytkowników:

1. Możliwość skonfigurowania za pomocą zmiennych w skrypcie co najmniej:
    a) ścieżki i nazwy pliku wejściowego
    b) ścieżki i nazwy pliku logującego
    c) ścieżki i nazwy pliku wyjściowego (właściwego skryptu)
    d) nazwy FQDN domeny
    e) nazwy NetBIOS domeny
    f) nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty
    g) ścieżki do udziału sieciowego HOME
    h) litery dysku katalogu domowego
2. Skrypt ma pobierać z pliku wejściowego listę kont użytkowników w formacie:
   NazwaUzytkownika;Imie;Nazwisko:Haslo;Dzial;NumerTelefonu
3. Skrypt tworzy nowe konta użytkowników w jednostce organizacyjnej

		nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu pobierając wszystkie niezbędne dane z pliku wejściowego 4. Nowo utworzone konta użytkowników muszą mieć jednorazowo ustawione hasła – użytkownik musi zmienić hasło podczas pierwszego logowania 5. Skrypt tworzy katalog \\DOMENA\HOME\NazwaUzytkownika 6. Skrypt nadaje uprawnienia do utworzonych katalogów użytkowników według założeń: a) Administratorzy Domeny – Pełna kontrola b) Użytkownik – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu NazwaUzytkownika c) Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu d) Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze 10. Skrypt ma ustawić dla każdego konta użytkownika literę dysku domowego oraz poprawną ścieżkę sieciową 11. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina) 12. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania 13. Skrypt ma wygenerować dla każdego zakładanego konta osobny plik tekstowy zawierający między innymi: Nazwę użytkownika, Imię, Nazwisko, Hasło do pierwszego zalogowania. Tak utworzone pliki mogą zostać wydrukowane i przekazane użytkownikom. Powyżej opisane skrypty muszą posiadać w treści kodu stosowne komentarze opisujące działanie skryptów. Skrypty zostanę przekazane Zamawiającemu w wieczyste użytkowanie bez dodatkowych opłat wraz ze stosowną dokumentacją użytkownika oraz szczegółową instrukcja obsługi. Zamawiający wymaga wygenerowania kont użytkowników, katalogów domowych użytkowników, jednostek organizacyjnych, grup zabezpieczeń za pomocą opracowanych skryptów.
17.	**Skonfigurowanie mapowania zasobów sieciowych**	Skonfigurowanie mechanizmów mapowania dysków sieciowych dla systemów klienckich Windows. Mapowane mają być między innymi zasoby: \\DOMENA\Public\SHARE1 \\DOMENA\Public\SHARE2 Oraz określone przez Zamawiającego drukarki sieciowe. Zamawiający wymaga skonfigurowanie mapowania dysków sieciowych za pomocą zasad grup na dwa sposoby: 1. Z wykorzystaniem skryptów logowania 2. Z wykorzystaniem mechanizmów zaimplementowanych w systemach Microsoft Windows Vista i nowszych (Wymagane jest także skonfigurowanie automatycznej instalacji niezbędnych składników na stacjach klienckich. Zamawiający nie dopuszcza instalacji wymaganych składników ręcznie).
17.	**Uruchomienie i skonfigurowanie serwera plików oraz**	Zamawiający wymaga uruchomienie oraz skonfigurowanie serwerów plików oraz serwerów wydruków tak, aby były spełnione poniższe założenia: Serwery plików muszą być skonfigurowane z wykorzystaniem dostępnych w

	wydruków	zaoferowanych systemach operacyjnych serwerów mechanizmów zwiększających dostępność danych poprzez zastosowanie technologii replikacji systemu plików. Konieczność taka podyktowana jest zapewnieniem ciągłości dostępu do krytycznych danych Wnioskodawcy w przypadku awarii jednego z serwera plików. Zastosowane mechanizmy replikacji systemu plików muszą zapewniać: • Replikację multi-master z rozwiązywaniem konfliktów • Wykorzystanie algorytmów kompresji danych wykrywających zmiany na poziomie bloków danych w obrębie plików – replikacji podlegają tylko zmienione bloki danych, a nie całe pliki. Serwery plików muszą być skonfigurowane w taki sposób, aby ograniczać ekspozycję danych dla użytkowników oraz grup, które nie mają do nich dostępu. Na serwerach plików muszą być skonfigurowana przydziały dyskowe dla użytkowników i grup. Zamawiający wymaga także skonfigurowania przydziałów dyskowych dla wskazanych folderów. Zamawiający wymaga włączenia i skonfigurowania mechanizmów uniemożliwiających przechowywanie niedozwolonych typów plików. Konieczne jest także skonfigurowanie mechanizmów raportujących. Zamawiający wymaga skonfigurowania mechanizmów przekierowania lokalnych folderów „Moje Dokumenty” oraz „Pulpit” ze stacji roboczych na serwery plików. Funkcjonalność ta musi poprawnie działać dla systemów klienckich Zamawiającego. Zamawiający wymaga stworzenie domyślnego, obowiązującego profilu wędrującego dla klienckich systemów operacyjnych. Domyślny profil ma uwzględniać opracowanie i wykonanie grafiki na pulpit komputera klienta. Grafika będzie akceptowana przez Zamawiającego. Zamawiający wymaga stworzenia i przypisania odpowiednich polityk globalnych dla wymuszenia stosowania obowiązkowych (niemodyfikowalnych) profili mobilnych. Zamawiający wymaga opracowania koszyka dozwolonych aplikacji wraz z implementacją polityk globalnych ograniczających dostęp do aplikacji z wykorzystaniem np.: dedykowanych ustawień związanych z polityką kontroli uruchomienia aplikacji. Zamawiający wymaga skonfigurowania parametrów audytu dla serwerów plików umożliwiających między innymi: a) Określenie daty, czasu, nazwy użytkownika, który usunął / próbował usunąć plik/folder b) Określenie daty, czasu, nazwy użytkownika, który zapisał / próbował zapisać plik/folder c) Określenia daty, czasu, nazwy użytkownika, który próbował uzyskać nieuprawniony dostęp do zasobów, do których nie ma uprawnień. Zamawiający wymaga uruchomienia serwera wydruków oraz podłączenia i skonfigurowania drukarek sieciowych. Zamawiający wymaga opracowania i skonfigurowania odpowiednich polityk globalnych mapujących odpowiednie drukarki użytkownikom. Niedopuszczalne jest przyłączenie wszystkim użytkownikom wszystkich dostępnych drukarek. Użytkownicy powinni mieć przyłączone drukarki znajdujące się najbliżej jego komputera.
17.	**Serwery uwierzytelniające**	1. Zamawiający wymaga uruchomienia serwerów uwierzytelniających współpracujących z infrastrukturą AD, realizujących funkcję uwierzytelniania na dostarczanych przełącznikach sieciowych. 2. Zamawiający wymaga uruchomienia co najmniej dwóch instancji serwera uwierzytelniania w celu zachowania redundancji na dwóch niezależnych

		serwerach. 3. Instancja serwera może być uruchomiona na serwerach domenowych z zastrzeżeniem, że będzie ona kompatybilna z usługami uruchomionymi na tych serwerach i nie będzie wpływać negatywnie na ich pracę. 4. Zamawiający wymaga skonfigurowania odpowiednich polityk bezpieczeństwa na zainstalowanych serwerach uwierzytelniających bazujących na utworzonych w strukturze usługi katalogowej Zamawiającego grupach. 5. Jeżeli jest potrzebna, Zamawiający wymaga dostarczenia licencji na instalowane serwery uwierzytelniające oraz ujęcia ich ceny w ofercie.
17.	**Uruchomienie usług umożliwiającą instalację i zarządzanie aktualizacjami stacji roboczych Windows**	Zamawiający wymaga uruchomienia i skonfigurowania usług dostępnych w dostarczonych systemach operacyjnych serwerów umożliwiających zarządzanie aktualizacjami stacji roboczych i serwerów Windows według założeń: 1. Aktualizacje i poprawki mają być pobierane na serwer instalacyjny za pośrednictwem sieci Internet 2. Administrator zatwierdza aktualizacje do instalacji 3. Stacje robocze i serwery pobierają i automatycznie instalują zatwierdzone przez Administratora aktualizacje według określonego harmonogramu Zamawiający wymaga skonfigurowania co najmniej następujących parametrów: 1. Systemów operacyjnych, aplikacji oraz wersji językowych, dla których będą pobierane aktualizacje 2. Kategorii aktualizacji 3. Grup komputerów (KOMPUTERY, SERWERY, KOMPUTERY-TEST, SERWERY-TEST) 4. Polityk globalnych przypisujących komputery znajdujące się w określonych jednostkach organizacyjnych do odpowiednich grup komputerów 5. Zasad automatycznego zatwierdzania nowych aktualizacji. 6. Mechanizmów raportowania (email)
17.	**Przygotowanie infrastruktury PKI**	Zamawiający wymaga przygotowania i uruchomienia wewnętrznej infrastruktury PKI. Zamawiający posiada stacje robocze pracujące w oparciu o następujące systemy operacyjne: Windows 10, 11. Wymagana przez Zamawiającego konfiguracja zawiera co najmniej: 1. Zaplanowanie i uruchomienie wewnętrznej struktury CA 2. Konfiguracja szablonów certyfikatów 3. Wydanie certyfikatów dla serwerów oraz stacji roboczych 4. Zastosowanie mechanizmów bezpieczeństwa poprzez możliwość backupu archiwizacji kluczy prywatnych wydawanych certyfikatów. 5. Wskazanie wszystkich możliwych dróg publikacji list CRL 6. Instalacji i konfiguracji stacji (komputer PC) do wydania kart – stacja do personalizacji.
18.	**Testowanie i modyfikacja parametrów infrastruktury sieciowej.**	1. Testowanie mechanizmów bezpieczeństwa klastra wirtualizacyjnego. 2. Testowanie wydajności przesyłu i zapisu danych do środowiska LAN. 3. Testowanie mechanizmów replikacji danych. 4. Testowanie dostępu publicznego do zasobów. 5. Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu 6. Testowanie autoryzowanego dostępu do wewnętrznych zasobów. 7. Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach
19.	**Asysty stanowiskowe**	Asysta stanowiskowa ma obejmować 16 godzin szkoleniowych w ujęciu 8 godzin na jeden dzień. Całość powinna się zamknąć w okresie 2 dni i ma dotyczyć autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia. Asysta musi być warunkiem dopuszczający do przekazania rozwiązania technicznego do wykorzystania produkcyjnego. Asysta stanowiskowa musi zostać odebrana i zatwierdzona protokołem odbioru sygnowanym przez obie strony projektu tj. wykonawcę oraz użytkownika końcowego.

20.	**Termin wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.**	Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą. **Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po pracach wdrożeniowo – instalacyjnych w godzinach od 8.00 do 15.30.** W tym czasie przedstawiciel Wykonawcy: • zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji. • dokona prezentacji działania sytemu dla pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności: a) zastosowanej technologii serwerów b) zastosowanej technologii pamięci masowej c) firewall/UTM d) sieci LAN e) systemu wirtualizacji/domeny (usługi katalogowej) f) systemu backupu g) zastosowanych rozwiązań aplikacyjnych Wykonawca zapewni również wparcie techniczne ze strony inżynierów w okresie trwania realizacji projektu. Wsparcie polegałoby na pomocy zdalnej lub telefonicznej przy rozwiązaniu problemów, które ewentualnie pojawią się podczas eksploatacji ww. rozwiązania.
21.	**Opracowanie dokumentacji powykonawczej**	Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu. 1. Wszelkie zmiany w stosunku do Dokumentacji systemu z podaniem ich powodów. 2. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację). 3. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały. 4. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały. 5. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów.