FORMULARZ OFERTOWY

|  |  |  |  |
| --- | --- | --- | --- |
| Wykonawca | |  | |
| Forma prowadzonej działalności | |  | |
| Adres | |  | |
| Adres do korespondencji | |  | |
| Województwo | |  | |
| NIP |  | Regon |  |
| Osoba upoważniona do kontaktów w sprawie oferty, telefon, e-mail | |  | |

Do:

Szpital Specjalistyczny im. J. Dietla w Krakowie

ul. Skarbowa 4,

31-121 Kraków

Nawiązując do zapytania cenowego dot. szacowania wartości wykonawca zgłasza swoją propozycję i wycenę na dostawę sprzętu komputerowego.

Warunki płatności: do 30 dni od daty otrzymania oryginału prawidłowo wystawionej faktury i po zrealizowaniu zamówienia potwierdzonego przez upoważnionego pracownika Zamawiającego.

Warunki gwarancji: 36 miesięcy NBD

Warunki dostawy: do siedziby zamawiającego w terminie 30 dni od podpisania umowy

Niniejsze zapytanie nie stanowi zapytania ofertowego w rozumieniu ustawy Prawo Zamówień publicznych, a uzyskane informacje posłużą wyłącznie do celów szacunkowych i planistycznych.

**Pakiet nr 1**

**Dostawa oprogramowania klasy EDR i AV wraz z wdrożeniem**

**Gwarancja/ licencje: 36 miesięcy**

CPV 48760000-3 - Pakiety oprogramowania do ochrony antywirusowej

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Przedmiot zamówienia** | **Ilość / jednostka miary** | **Cena jednostkowa netto** | **Stawka VAT** | **Cena jednostkowa brutto** | **Wartość netto** | **Wartość brutto** |
|  | **Dostawa oprogramowania antywirusowego (AV)** | 430 szt |  |  |  |  |  |
|  | **Dostawa oprogramowania klasy EDR (Endpoint Detection & Response)** | 430 szt/3lata |  |  |  |  |  |
|  | **Instalacja oprogramowania na wskazanych stacjach**  **Instalacja oprogramowania do zarządzania EDR/AV** | Pakiet |  |  |  |  |  |
|  | **Szkolenia** | 8 osób |  |  |  |  |  |
|  | **Opracowanie polityki zarządzania EDR+AV w szpitalu** | Pakiet |  |  |  |  |  |

**Pakiet 2**

**Dostawa Przełączników sieciowych wraz z konfiguracją**

**Gwarancja/ licencje: 36 miesięcy**

**CPV: 32422000-7 -Elementy składowe sieci**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Przedmiot zamówienia** | **Ilość / jednostka miary** | **Cena jednostkowa netto** | **Stawka VAT** | **Cena jednostkowa brutto** | **Wartość netto** | **Wartość brutto** |
|  | **Przełączniki sieciowe A** | 15 szt |  |  |  |  |  |
|  | **Przełączniki sieciowe B** | 40 szt |  |  |  |  |  |
|  | **Wdrożenie i wykonanie dokumentacji** | 1 |  |  |  |  |  |
|  | **Szkolenia** | 6 osób |  |  |  |  |  |
|  | **Wymagania dodatkowe (oceniane)** | Licencja 3 lata |  |  |  |  |  |

**Pakiet 3**

**Dostawa środowiska backupowego**

**Gwarancja/ licencje: 36 miesięcy**

CPV- 48710000-8 Pakiety oprogramowania do kopii zapasowych i odzyskiwania

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Przedmiot zamówienia** | **Ilość / jednostka miary** | **Cena jednostkowa netto** | **Stawka VAT** | **Cena jednostkowa brutto** | **Wartość netto** | **Wartość brutto** |
|  | Urządzenie z deduplikacja | 1 szt |  |  |  |  |  |
|  | Serwer do backupu | 1 szt |  |  |  |  |  |
|  | Oprogramowanie do backupu | 1 szt |  |  |  |  |  |
|  | Szkolenia | 6 osób |  |  |  |  |  |
|  | Wdrożenie i wykonanie dokumentacji | 1 szt |  |  |  |  |  |
|  | Środowisko do przechowywania odseparowanej kopi zapasowej | 3 lata/1 szt. |  |  |  |  |  |
| **Razem:** | | | | | |  |  |

**Pakiet 4**

**Dostawa Systemu do zarządzania zasobami IT w Szpitalu**

**Gwarancja/ licencja: 36 miesięcy**

**CPV:** 48781000-6 Pakiety oprogramowania do zarządzania systemem

72250000-2 Usługi w zakresie konserwacji i wsparcia systemów

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Przedmiot zamówienia** | **Ilość / jednostka miary** | **Cena jednostkowa netto** | **Stawka VAT** | **Cena jednostkowa brutto** | **Wartość netto** | **Wartość brutto** |
|  | Oprogramowanie do zarządzania | 1 szt |  |  |  |  |  |
|  | Szkolenia | 6 osób |  |  |  |  |  |
|  | Wdrożenie i wykonanie dokumentacji | 1 szt |  |  |  |  |  |
| **Razem:** | | | | | |  |  |

**Pakiet nr 1**

**Wymagania**

1. Jeden producent rozwiązania EDR i AV
2. Oprogramowanie AV musi być testowane pod względem wydajności np. z wykorzystaniem UL Procyon® Benchmark-Suite zgodnie z metodologią testów opartą na <https://benchmarks.ul.com/procyon/office-productivity-benchmark> lub inną równoważną dla Windows 10/11. Poprzez równoważną metodologię testów Zamawiający rozumie:

* test wykonany w oparciu o typowe zadania i wzorce pracy biurowej pakietu Office,
* test porównawczy wykonuje zadania z arkuszami programu Excel, prezentacjami programu PowerPoint, dokumentami programu Word i wiadomościami e-mail programu Outlook otwartymi w tym samym czasie,
* aplikacje te pozostają uruchomione w tle, gdy uwaga przenosi się z jednego zadania na drugie. Przykładowy scenariusz kopiowanie wykresów z programu Excel i dodawanie ich do slajdu programu PowerPoint lub porównywanie i przenoszenie treści między dokumentami programu Word,
* test jest kompatybilny z pakietami Office 2019 / 2021 i Microsoft 365,
* testy zostały wykonane min 3 - krotnie, aby wyeliminować wpływ SO.

Wyniki MUSZĄ być większe niż 90%. Rozwiązania dla których wynik będzie mniejszy niż 90% zostaną odrzucone. Testy musza być przeprowadzone po 1 lipca 2025 r.

Wynik testów wydajności:

|  |  |  |
| --- | --- | --- |
| Nazwa programu AV/wersja | Wynik w testach wydajności | Dokument potwierdzający wynik |
|  | Wynik ≥ 90%  *Podać* | nazwa dokumentu dołączona do oferty (zaleca się dołączyć dokument w formacie PDF) |

Testy przeprowadzone przez av-comparatives.org (<https://www.av-comparatives.org/tests/performance-test-september-2025/>)

W przypadku braku wyniku na w/w stronie Wykonawca dostarczy własne wyniki przeprowadzonych testów (zaleca się w formacie PDF) lub link do innych niezależnych badań wydajności. Zamawiający zastrzega sobie prawo do ich weryfikacji.

W przypadku wykonania własnych testów wyniki musza zawierać:

- informacje o oprogramowaniu użytym do przeprowadzenia testów zgodnych z metodologią opisaną na stronie <https://benchmarks.ul.com/procyon/office-productivity-benchmark>,

- sprzęcie, na którym zostały przeprowadzone w/w testy,

- dacie wykonania testów,

- nazwie instytucji wykonującej test.

**Urządzenia podlegające ochronie AV i EDR.**

1. Ochrona antywirusowa stacji roboczych: 430 szt.

* Microsoft Windows 10
* Microsoft Windows 11

1. Ochrona serwerów: 30 szt.

* Windows 2012 R2 standard
* Windows Serwer 2019
* Windows Serwer 2022 Standard Evaluation 21H2
* Linux Debian 11
* Oracle Linux Serwer 8.7

**I. Dostawa oprogramowania antywirusowego (AV)**

**Wymagania oprogramowania antywirusowego/antyspyware**

1. Polski lub angielski interfejs użytkownika i dokumentacja do oprogramowania.
2. Ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
4. Wykrywanie zagrożeń i analiza procesów technikami behawioralnymi.
5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6. Wbudowana technologia do ochrony przed rootkitami.
7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Możliwość skanowania całego dysku, „na żądanie” z poziomu użytkownika końcowego wybranych katalogów lub pojedynczych plików.
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
11. Opcjonalna możliwość skanowania dysków sieciowych i dysków przenośnych.
12. Skanowanie zarówno plików spakowanych i skompresowanych, ale również możliwość skanowania plików niespakowanych i nieskompresowanych.
13. Ochrona krytycznych kluczy rejestru przed ich wykorzystaniem lub nieautoryzowanym dostępem do nich.
14. Możliwość dodawania wykluczeń na podstawie:
    1. Plik / Folder
    2. Rozszerzenie
    3. Proces
    4. Hash pliku
    5. Hash certyfikatu
    6. Nazwa zagrożenia
    7. Wiersz poleceń
    8. IP/maska
15. W GUI programu na punkcie końcowym z systemem Windows możliwość wyświetlenia aktualnej wersji produktu.
16. W GUI programu na punkcie końcowym z systemem Windows możliwość wyświetlenia, kiedy była przeprowadzana ostatnie połączenie do konsoli z dokładnością co do dnia i godziny.
17. Automatyczna, inkrementacyjna weryfikacja zawartości danych na podstawie, których agent realizuje ochronę.
18. Administrator musi mieć możliwość ukrycia ikony oprogramowania w obszarze powiadomień systemu Windows.
19. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na punkcie końcowym Windows.
20. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
21. Oprogramowanie klienckie posiada wbudowaną funkcję do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
22. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
23. Możliwość tworzenia list sieci zaufanych.
24. Możliwość dezaktywacji funkcji zapory sieciowej.
25. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
26. Komunikacja między konsolą zarządzającą, a punktami końcowymi jest szyfrowana.
27. Wbudowana ochrona przed exploitami musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technika eksploatacji. Funkcja umożliwia również:
    * 1. Przekierowanie APC
      2. Obejście Data Execution Prevention
      3. DLL Hijacking
      4. Exploit Kit Fingerprinting
      5. JIT
      6. Null Dereference
      7. ROP
      8. Structures exception handler hijackings
      9. Heap Spray
      10. Kernel Privilege Escalation.
28. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak:
    1. Pierwszy dostęp.
    2. Dostęp do poświadczeń.
    3. Wykrycie.
    4. Crimeware.
29. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym.
30. Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności w systemie Windows.
31. System musi posiadać możliwość kontroli urządzeń podłączanych do portów USB co najmniej na systemach windows i macOS w następującym zakresie:

a) Określenia jakie urządzenia USB można podłączyć

b) Określenia zakresu dostępu do pamięci masowej USB:

c) Brak dostępu

d) Tylko odczyt

e) Odczyt i zapis

f) Odczyt, zapis i uruchamianie.

1. System musi umożliwiać skanowanie oprogramowania układowego UEFI.
2. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników naruszeń bezpieczeństwa (IOC).
3. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego administratora, przy próbie deinstalacji program powinien pytać o hasło.

**Wymagania dotyczące zdalnej konsoli administracyjnej**

* + - 1. Ochrona antywirusowa monitorowana i zarządzana z pojedynczej, centralnej konsoli.
      2. Możliwość zarządzania stacjami końcowymi z poziomu konsoli w modelu SaaS dostarczonej wraz z zaproponowanym rozwiązaniem.
      3. Konsola musi umożliwiać centralne zarządzanie i konfigurację ochrony wspieranych stacji roboczych i serwerów.
      4. Centralny System musi umożliwiać centralne zarządzanie i konfigurację ochrony wspieranych stacji roboczych i serwerów
      5. Możliwość uruchomienia zdalnego skanowania wybranych punktów końcowych
      6. Możliwość utworzenia konta użytkownika z rolą administrator lub z ustawieniami niestandardowymi.
      7. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, systemu operacyjnego.
      8. Możliwość włączenia blokowania określonych zewnętrznych nośników danych na określonej stacji w tym przynajmniej:

1. Dyski
2. Napędy CD-ROM
3. Przenośne urządzenia systemu Windows (Windows Portable Devices)
4. Napędy dyskietek
5. Zadania drukowania (Print Jobs)
6. Urządzenia Bluetooth.
   * + 1. Możliwość centralnej aktualizacji punktów końcowych z serwera w sieci lokalnej lub z Internetu.
       2. System musi posiadać możliwość skonfigurowania manualnej i automatycznej aktualizacji agenta dla wskazanych grup endpointów. Polityka automatycznej konfiguracji agenta musi umożliwiać określenie:

a) Dnia tygodnia i zakresu czasu, w którym aktualizacja nie będzie wykonywana

b) Liczby aktualizowanych endpointów

c) Możliwość zdefiniowania wersji: najnowsza wersja, najnowsza przedostatnia wersja, statycznie wskazana wersja.

* + - 1. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
      2. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) oraz wyeksportowanie ich do formatu**: pdf** lub **csv**.
      3. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie.
      4. Możliwość generowania raportu maksymalnie raz na 24 godziny.
      5. Pierwsza aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
      6. Możliwość dodania etykiety do stacji roboczej.
      7. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji. Określenie lokalizacji na podstawie:

1. Zakres adresów IP/IP.
2. Nazwa hosta.
   * + 1. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Przypisywanie musi odbywać się ręcznie lub automatycznie. Musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
       2. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony punktu końcowego (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania na żądanie, zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
       3. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238.
       4. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
       5. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
       6. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux.
       7. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
       8. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows lub Linux.
       9. System umożliwia pobieranie raportów o plikach poddanych kwarantannie z poziomu centralnej konsoli administracyjnej.
       10. Ochrona proaktywna oparta o maszynowe uczenie, która działa w fazie poprzedzającej wykonanie. Ochrona ta musi wykrywać zagrożenia takie jak:
3. Ukierunkowane ataki.
4. Podejrzane pliki i ruch w sieci.
5. Exploity.
6. Ransomware.
7. Grayware.
   * + 1. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego.
       2. Zintegrowany sandbox po stronie producenta, który pozwala na analizę pliku. Plik może zostać wysłany automatycznie ze stacji roboczej, jeżeli oprogramowanie uzna go za podejrzany lub z poziomu konsoli przez administratora.
       3. Rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa
8. Minimalny - 1KB.
9. Maksymalny - 100MB.
   * + 1. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według minimum:
10. daty,
11. kategorii,
12. typu zagrożenia,
13. działań naprawczych.
    * + 1. Możliwość aby dla lokalnych kont podczas tworzenia haseł dla kont administracyjnych musi żądać stosowania się do przyjętej polityki, która wymaga ustawienia hasła spełniającego następujące kryteria: co najmniej 11 znaków, musi zawierać małe i duże litery łacińskie, cyfry i znaki specjalne.
        2. System musi posiadać mechanizmy blokowania konta po przynajmniej 5 niepoprawnych próbach podania hasła.
        3. Możliwość zablokowania konta w konsoli, jeżeli użytkownik tego konta próbował logować się nieprawidłowym hasłem.
        4. Raport podsumowujący - Możliwość podglądu raportu, który streszcza stan środowiska firmowego w ciągu ostatnich 24h, 7 dni lub 30 dni. Z rozróżnieniem na takie sekcje jak:
14. Zarządzane punkty końcowe.
15. Ilość zajętych miejsc w licencji z rozróżnieniem na stacje robocze Windows, serwery Windows/Linux oraz fizyczne punkty końcowe i maszyny wirtualne.
16. najczęściej blokowanych zagrożenia
17. Podział zagrożeń na urządzenia takie jak stacje robocze i serwery.
18. Status incydentów bezpieczeństwa, które wystąpiły.
19. Stan modułów punktów końcowych.
20. Zablokowane techniki ataku sieciowego z podziałem na takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware.
    * + 1. System musi posiadać funkcję wstrzymywania skanowania podczas pracy na baterii.
        2. Filtrowanie wykrytych incydentów bezpieczeństwa m.in. na podstawie: (musi spełniać min 5 warunków z poniższej listy)
21. Status/Stan.
22. Osoba.
23. Czas utworzenia.
24. Priorytet.
25. Ostatnia faza killchain.
26. Wykonane czynności.
27. Skorelowane incydenty.
28. Typ incydentu.
29. Stopień zagrożenia.
30. Nazwa.
31. Tagi.
    * + 1. System musi zbierać co najmniej następujące dane telemetryczne z wskazanych systemów operacyjnych :
           1. Windows

Utworzenie nowego procesu i zakończenie procesu

Wszystkie operacje na plikach: tworzenie, zapisywanie, kasowanie, zmiana nazwy, przesunięcie, modyfikacja, link symboliczny

Ładowanie bibliotek DLL

Wstrzykiwanie do procesu

Wszystkie operacje na socketach sieciowych dla TCP i UDP: accept, connect, create, listen, close, bind

Statystyki połączeń sieciowych

Praca z rejestrem: skasowanie wartości, ustawienie wartości, utworzenie klucza, kasowanie klucza, zmiana nazwy klucza.

* + - * 1. Linux

Utworzenie nowego procesu i zakończenie procesu.

Informacje o kontenerach (co najmniej docker i containerd).

Wszystkie operacje na socketach sieciowych dla TCP i UD: listen, accept, connect, connect failure, disconnect

* + - 1. Oprogramowanie musi zbierać co najmniej następujące dane telemetryczne:

1. Utworzenie nowego procesu i zakończenie procesu
2. Wszystkie operacje na plikach: tworzenie, zapisywanie, kasowanie, zmiana nazwy, przesunięcie, modyfikacja, link symboliczny
3. Ładowanie bibliotek DLL
4. Wstrzykiwanie do procesu
5. Wszystkie operacje na socketach sieciowych dla TCP i UDP: accept, connect, create, listen, close, bind
6. Statystyki połączeń sieciowych
7. Praca z rejestrem: skasowanie wartości, ustawienie wartości, utworzenie klucza, kasowanie klucza, zmiana nazwy klucza.

**II. Dostawa oprogramowania EDR (Endpoint Detection & Response)**

**Komponenty EDR**

1. Sensor EDR, który gromadzi i przetwarza dane dotyczące punktu końcowego i zachowania aplikacji w celu ich raportowania.
2. Konsola centralna (Analityka Bezpieczeństwa) - komponent służący do interpretacji metadanych gromadzonych przez sensor EDR oraz współpracujący z systemem AV.
3. Przesyłanie informacji serwer-agent powinno być zabezpieczone przy użyciu protokołu SSL

**Wykrywanie podejrzanej aktywności**

1. Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności.
2. Bazowanie na systemach opartych o techniki MITRE ATT&CK i własnej inteligencji.
3. Zgłaszanie naruszeń jako incydent w module EDR.
4. Posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikalnego identyfikatora sprzętowego stacji.

**Badanie incydentów i wizualizacja**

1. Konsola centralna działa o oparciu o serwis WWW.
2. System posiada możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej funkcje zarządzania:
3. Politykami,
4. Raportowaniem,
5. Zadaniami administracyjnymi.

Każda z powyższych funkcji posiada możliwość wyboru uprawnienia: odczyt, zapisz, brak.

1. Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym czasie.
2. Produkt integruje się z bazą wiedzy MITRE ATT&CK i odpowiednio oznacza zdarzenia bezpieczeństwa.
3. Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi danymi lub działaniami z następującymi informacjami:
4. Karta podsumowująca zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia.
5. Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej.
6. System gromadzi informacje o działaniach podejmowanych przez produkt w związku ze zdarzeniem bezpieczeństwa.

**Incydenty**

1. Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i chronologicznej linii zdarzeń lub daje możliwość:
2. Filtrowania zdarzeń.
3. Zakończenia procesów.
4. Dodania procesów do czarnej listy.
5. Dodania procesów do białej listy.
6. Izolacji hosta.
7. automatycznego przesyłania pliku do Sandbox.
8. Sprawdzenia informacji o pliku w VirusTotal.
9. Możliwość szybkiego podglądu incydentów za pomocą spersonalizowanych widoków list lub widoku domyślnego.
10. System umożliwia blokowanie na podstawie utworzonych reguł czarnej listy przy pomocy SHA256.
11. Możliwość wskazania lisy reguł dla czarnej listy dla konkretnych HASH.
12. System musi oferować szeroki zakres filtrowania dodanych reguł blokowania minimum po nazwie pliku, hash pliku, typu hash256.

**III. Instalacja oprogramowania na wskazanych stacjach**

W ramach prac instalacyjnych Wykonawca wykona instalacji oprogramowania AV i EDR na:

1. Na wskazanych stacjach (minimum 30 szt)
2. Na serwerach i środowiskach wirtualnych (30 szt)

Wykona parametryzację i ustawienia oprogramowania do optymalnej pracy (best practics)

**IV. Instalacja oprogramowania do zarządzania EDR/AV**

* + - 1. Instalacja zdalnej konsoli administracyjnej (6 stanowisk)
      2. Konsola centralna EDR (6 stanowisk)
      3. Konfiguracja oprogramowania
      4. Założenie kont administratorów (6 osób)

V. **Przeszkolenie personelu**

1. Szkolenie dla administratorów, minimalny zakres:
2. Instalacja i ustawienie programu AV
3. Instalacja i ustawienia sensora EDR
4. Analiza danych
5. Tworzenie raportów
6. Konfiguracja konsoli i kont administratorów i użytkowników
7. Korzystanie z zaawansowanych funkcji oprogramowania m.in. Sandbox,
8. zarządzanie incydentami
9. zarządzanie podatnościami
10. tworzenie reguł i polityk
11. Ilość osób do przeszkolenia 8 w 2 grupach po 4 osoby (łącznie 4 dni)
12. Czas szkolenia 6 h
13. Teoria 3 h
14. Warsztaty 3h
15. Przygotowanie broszury z ważnymi informacjami użytkowymi dla użytkowników komputerów
    * 1. **Opracowanie polityki zarządzania EDR+AV w szpitalu**

Zakres opracowania:

- opis stanu po wdrożeniu;

- osoby odpowiedzialne;

- procedura reagowania na incydenty (w tym dokumenty, raporty, osoby odpowiedzialne);

- raportowanie do Dyrekcji;

- dokumentowanie pracy systemu;

**Pakiet nr 2**

**Opis:**

**Przełączniki sieciowe A**

Urządzenie dostarczone jest z oficjalnej dystrybucji producenta przeznaczonej na teren Unii Europejskiej.

|  |  |  |
| --- | --- | --- |
| **Producent** | |  |
| **Model** | |  |
| **Nazwa wymagania** | **Minimalne parametry** | **Oferowane parametry** |
| **Przełącznik zarządzalny klasy L2/L3** | | |
| **Wysokość** | Max 2U 19” |  |
| **Porty** | Min 48 portów Gigabit  Min 4 porty SFP+ |  |
| **PoE** | TAK min PoE+ (802.3at) |  |
| **Łączna moc PoE** | Min 400W |  |
| **Tablica MAC** | min. 16K |  |
| **Przepustowość 64 B** | min. 120 Mpps |  |
| **Porty (zarządzanie)** | min. 1 x USB  port konsoli RJ45 |  |
| **Zarządzanie** | Out-of-band  IT Web GUI (main)  HTTPs  CLI;  Telnet;  SNMP,  MIBs RSPAN  Radius Users,  TACACS+ |  |
| **Bezpieczeństwo** | ACL (L2/L3)  QoS  DiffServ  IPv4/IPv6 Multicast filtering  IGMPv3 MLDv2 Snooping  DOT1X / MAB  IPv4 / IPv6 Static Routing (port, podsieć, VLAN)  Control Packet Flooding |  |
| **VLAN** | Min 4000  Static,  Dynamic,  Voice,  MAC,  Double VLAN mode,  Private VLANs  Trunking Port Channel |  |
| **Oprogramowanie Centralne** | Możliwość zarządzania urządzeniem przez centralne oprogramowanie. |  |
| **Dodatkowe wyposażenie** | Do każdego przełącznika Wykonawca dostarczy zestaw (2 szt.) modułów światłowodowych SFP+ 10Gb/s Multi Mode LC duplex o zasięgu 100 m |  |

Dodatkowo Wykonawca w cenie oferty dostarczy 4 zestawy wkładek SFP+

SingleMode 1270nm/1330nm 20km Simplex, typ złącza LC/UPC, kodowanie Cisco. Wszystkie moduły SFP+ muszą być w pełni kompatybilne z dostarczanymi urządzeniami.

**Przełączniki sieciowe B**

|  |  |  |
| --- | --- | --- |
| **Producent** | |  |
| **Model** | |  |
| **Nazwa wymagania** | **Minimalne parametry** | **Oferowane parametry** |
| **Przełącznik zarządzalny klasy L2/L3** | | |
| **Porty** | Min 8 portów Gigabit |  |
| **Wymiary** | Suma wymiarów (Wys+Szer+ Gł)<600mm |  |
| **Tablica MAC** | min. 16K |  |
| **Przepustowość 64 B** | min. 14 Mpps |  |
| **Porty (zarządzanie)** | min. 1 x USB  port konsoli RJ45 |  |
| **Zarządzanie** | Out-of-band  IT Web GUI (main)  HTTPs  CLI;  Telnet;  SNMP,  MIBs RSPAN  Radius Users,  TACACS+ |  |
| **Bezpieczeństwo** | ACL (L2/L3)  QoS  DiffServ  IPv4/IPv6 Multicast filtering  IGMPv3 MLDv2 Snooping  DOT1X / MAB  IPv4 / IPv6 Static Routing (port, podsieć, VLAN)  Control Packet Flooding |  |
| **VLAN** | Min 4000  Static,  Dynamic,  Voice,  MAC,  Double VLAN mode,  Private VLANs  Trunking Port Channel |  |
| **Oprogramowanie Centralne** | Możliwość zarządzania urządzeniem przez centralne oprogramowanie. |  |

* + - 1. **Wdrożenie i wykonanie dokumentacji**

Wykonawca w ramach wdrożenia:

Dostarczy, wstępnie skonfiguruje przełączniki, zainstaluje we wskazanych miejscach,

Wspólnie z przedstawicielami opracuje koncepcję segmentacji sieci,

Skonfiguruje przełączniki (routing, segmentacja, bezpieczeństwo) zgodnie z ustaleniami,

Wykona dokumentację powdrożeniową w wersji elektronicznej (PDF, DOCX, XLSX):

Schemat logicznych połączeń,

Adresację,

Konfigurację,

Polityka zarządzania siecią komputerową:

* Monitorowanie sieci;
* Zarządzanie konfiguracją;
* Zarządzanie wydajnością;
* Zarządzanie bezpieczeństwem;
* Zarządzanie incydentami;
* Planowanie pojemności;
  + - 1. **Szkolenia**

Ilość osób do szkolenia: 6 (2 grupy po 3 osoby).

Każda z grup ma odbywać szkolenie w innym terminie (rozłącznym)

Szkolenie powinno trwać min 6h w tym:

* min. 2 godziny teorii
* min. 3 godziny warsztatu

Szkolenie musi odbyć się w ośrodku szkoleniowym znajdującym się na terenie Krakowa

Szkolenie musi być prowadzone w języku polskim

Szkolenie musi być prowadzone przez oficjalnych partnerów, trenerów i dostawców szkoleń, którzy przeszli weryfikację producenta urządzeń

Szkolenie musi obejmować:

* Konfigurację urządzeń
* Backup konfiguracji
* Konfigurację vlan
* Routing
* Konfigurację portów
* Konfigurację powiadomień i raportów

Wykonawca zapewni dla każdego uczestnika wersję elektroniczną materiałów dydaktycznych zawierających streszczenie/omówienie wszystkich zagadnień zawartych w programie szkolenia oraz wykorzystane prezentacje

Wykonawca po zakończeniu szkolenia wystawi uczestnikom dokument/certyfikat potwierdzający odbycie szkolenia wraz z jego zakresem.

* + - 1. **Wymagania dodatkowe (oceniane).**

Dostawa oprogramowania do centralnego zarządzania siecią.

W przypadku zaoferowania oprogramowania opisanego poniżej Wykonawca otrzyma **40 pkt.**

Wykonawca, aby otrzymać 40 punktów w tym kryterium musi dostarczyć oprogramowanie spełniające WSZYSTKIE wymagania Zamawiającego. W przypadku gdy zaoferowane oprogramowanie nie będzie spełniało poniższych wymagań oferta otrzyma 0 punktów.

**Wymagania dotyczące oprogramowania:**

|  |  |  |
| --- | --- | --- |
| **Producent** | |  |
| **Nazwa oprogramowania** | |  |
| **Parametr** | **Wymagany** | **Proponowany** |
| **Wizualizacja** | Interaktywna mapa połączeń pomiędzy urządzeniami przedstawiana w czasie rzeczywistym wraz z identyfikacją i klasyfikacją urządzeń. |  |
| **Konfiguracja** | - Centralna baza konfiguracji wszystkich urządzeń sieciowych.  - Możliwość grupowej konfiguracji urządzeń sieciowych. |  |
| **Monitorowanie** | Centralne repozytorium logów, alarmów i informacji o zmianach na urządzeniach i w topologii sieci.  System monitorowania usług sieciowych i aplikacji pod względem ich wykorzystania. |  |
| **Bezpieczeństwo** | - Tworzenie i zarządzanie polityką bezpieczeństwa w dostępie do sieci dla grup urządzeń oraz użytkowników.  - System kontroli dostępu do sieci w oparciu o IEEE 802.1X. |  |
| **Integracja** | Zarządzanie urządzeniami dostarczonymi oraz posiadanymi przez Zamawiającego przełącznikami core, urządzeniami UTM |  |
| **Interface** | Integracja z systemami firm trzecich API, minimum z centralną baza logów. |  |
| **Autoryzacja** | RADIUS  TACACS+. |  |
| **Licencja na w/w funkcje** | 3 lata na wszystkie funkcjonalności |  |

W przypadku dostarczenia oprogramowania do zarządzania siecią, wykonawca dostarczy przed podpisaniem protokołu odbioru dokumentację tj. instrukcję użytkownika oraz dokumentację techniczną programu z uwzględnieniem dokumentacji integracyjnej API.

**Pakiet nr 3**

Przedmiotem zamówienia jest zakup i wdrożenie systemu do tworzenia kopii zapasowych (backup) składającego się z:

1. Urządzenie do wykonywania kopii zapasowych
2. Oprogramowania do wykonywania backupu
3. Środowiska do przechowywania odseparowanej kopii zapasowej (chmura lub rozwiązanie równoważne)

W ramach dostawy wykonawca:

1. Wykona montaż, instalację i konfigurację sprzętu i oprogramowania
2. Przeszkoli personel w zakresie:
   1. Obsługi oprogramowania
   2. Wykonywania kopii zapasowych
   3. Odtwarzania i weryfikacji kopii zapasowych
3. Opracuje dokumenty:
   1. Dokumentacja powdrożeniowa systemu backupu
   2. Polityki i Procedury
   3. Plan Odtwarzania Awaryjnego
      * 1. **Urządzenie do wykonywania kopii zapasowych – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **Nazwa wymagania** | **Wymagania minimalne** | **Parametry oferowane** |
| Obudowa | * Obudowa rack rozmiar: 2U |  |
| Przestrzeń dyskowa | Urządzenie musi oferować pojemność minimum 42 TB netto po RAID 6  W pojemność Urządzenia nie może wliczać się przestrzeń znajdująca się w chmurze (tzw. Cloud). |  |
| Procesor | Procesor: min. 8 rdzeni, min. 16 wątków. Minimalna częstotliwość bazowa procesora 2.6GHz |  |
| Pamięć RAM | Pamięć RAM: 32GB |  |
| Interfejsy | Min. 2szt. Ethernet 1 Gb, Dual SFP28 |  |
| Dyski systemowe | Osobne dyski SSD M.2 nVME działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego |  |
| Zasilanie | Urządzenie musi posiadać redundantne zasilanie |  |
| Gwarancja | Gwarancja NBD on-premise obowiązująca przez min. 36 miesięcy |  |
| Data produkcji | Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2025r. |  |
| Integracja z systemami backup | Urządzenie musi współpracować z oprogramowaniem do zarządzania kopiami bezpieczeństwa dostarczonymi w tym postępowaniu. |  |
| Dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. |  |
| Warunki gwarancji | Zachowanie dysków (zatrzymanie uszkodzonych nośników w przypadku ich awarii) |  |
| Bezpieczeństwo | Urządzenie w korelacji z oprogramowaniem musi zapewniać bezpieczeństwo przed atakami ransomware. Urządzenie musi być rozwiązaniem specjalistycznym i służyć tylko do obsługi systemu backupowego (wykonywanie backupu, przechowywanie backupu, przywracanie backupu). |  |
| System | Urządzenie powinno być dostarczone w ramach appliance z zainstalowanymi i skonfigurowanymi usługami, niezbędnymi do pracy systemu. Nie dopuszcza się otwartych systemów NAS. |  |

* + - 1. **Oprogramowania do wykonywania backupu i odzyskiwania danych**

Ilość maszyn fizycznych: 15

Ilość maszyn wirtualnych: 15

Ilość stacji roboczych do backupu: 40

Wymagania:

1. Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia oprogramowania do zabezpieczania środowiska Data Center Zamawiającego (baz danych, maszyn wirtualnych, serwerów plików, serwerów wolnostojących) zwanego dalej oprogramowaniem.
2. Wymagane jest dostarczenie wszystkich modułów oprogramowania tak, aby zapewnić backup całości wyspecyfikowanego środowiska oraz spełnić wszystkie wymienione w niniejszej tabeli funkcjonalności.

**Wspierane systemy**

Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:

Alpine 3.10+,

Debian: 9+,

Ubuntu: 16.04+,

Fedora: 29+,

centOS: 7+,

RHEL: 6+,

openSUSE: 15+,

SUSE Enterprise Linux(SLES): 12 SP2+,

macOS: 10.13+,

Windows: 7, 8.1, 10(1607+),

Windows Server: 2008 R2+,

Środowisk wirtualnych:

Hyper-V 2016+,

VMware: 6.7+.

**Zarządzanie i magazyny**

1. Produkt dostępny w polskiej wersji językowej.
2. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
3. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków
4. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów
5. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych
6. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
7. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
8. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe
9. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
10. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
11. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
12. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.
13. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
14. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
15. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.
16. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
17. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
18. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
19. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych
20. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
21. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
22. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
23. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
24. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
25. System powinien umożliwiać wysyłanie powiadomień  o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,
26. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
27. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.
28. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
29. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
30. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
31. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych
32. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
33. Proces deduplikacji realizowany jest blokiem o zmiennej wielkości. Wielkość ta ustalona jest dynamicznie w trakcie wykonywania kopii zapasowej w celu zapewnienia jak najwyższej efektywności procesu.
34. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
35. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
36. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
37. System musi pozwalać na automatyczne aktualizacje oprogramowania.
38. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
39. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.
40. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
41. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
42. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
43. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
44. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
45. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
46. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
47. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
48. System kopii zapasowej musi umozliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
49. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
50. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental,
51. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
52. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3 oraz dedykowana chmura producenta appliance’u
53. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb,S3, nfs, iscsi, katalog lokalny
54. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).
55. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.
56. Możliwość generowania raportów dobowych w oparciu o harmonogram
57. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter powinno być zlokalizowane na terenie Polski)
58. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)
59. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.
60. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)

**Wymagania dotyczące backupu serwerów zwirtualizowanych**

1. Oprogramowanie do musi współpracować z infrastrukturą VMware w wersji 7.0, 8.1
2. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
3. Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere.
4. System musi wspierać kopię w trybie application-aware dla wirtualizatorów Hyper-V oraz vSphere.
5. 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.
6. Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
7. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
8. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu webowym.
9. 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.
10. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
11. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
12. Oprogramowanie musi wspierać kopiowanie backupów na taśmy
13. Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej.
14. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
15. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).
16. Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli
17. Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing).
18. Oprogramowanie musi umożliwiać uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny.
19. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
20. Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
21. Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs,
22. Windows: NTFS, FAT, FAT32, ReFS.
23. Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
24. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku dla wybranych wirtualizatorów.
25. Rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
26. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.
27. System musi wspierać kopię w trybie application-aware dla wirtualizatorów Hyper-V oraz vSphere.

**Wymagania dotyczące backupu serwerów zwirtualizowanych**

1. Oprogramowanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.
2. Oprogramowanie musi wspierać Windows 10 lub nowsze (dotyczy stacji roboczych) oraz Windows Server 2012 lub nowsze (dotyczy serwerów).
3. Oprogramowanie musi wspierać Linux kernel 2.6.32 lub nowsze (zarówno 32 jak i 64bit) oraz wspierać następujące dystrybucje: Debian 10 lub nowsze.
4. Oprogramowanie musi mieć możliwość instalacji oraz zarządzania poprzez centralną konsolę zarządzającą.
5. Oprogramowanie musi wspierać systemy oparte o Microsoft Failover Cluster.
6. Oprogramowanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów,
7. Oprogramowanie musi wspierać backup podłączonych dysków USB.
8. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym.
9. Oprogramowanie musi pozwalać na przechowywanie kopii zapasowych na:
   1. Lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny.
   2. Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire.
   3. Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS.
   4. Zcentralizowanym repozytorium danych.
   5. Bezpośrednio na zasobach Chmury.
10. Oprogramowanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone.
11. Oprogramowanie musi wspierać kontrolę pasma sieciowego.
12. Oprogramowanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN.
13. Oprogramowanie musi wspierać technologię BitLocker.
14. Oprogramowanie musi wspierać uruchamianie z nośnika odtwarzania. Nośnik odtwarzania musi być automatycznie tworzony przez oprogramowanie.
15. Oprogramowanie musi wspierać wgrywanie dodatkowych sterowników podczas odtwarzania z wykorzystaniem nośnika odtwarzania.
16. Oprogramowanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.
17. Oprogramowanie musi wspierać szyfrowanie.
18. Oprogramowanie musi wspierać tworzenie wielu zadań backupowych.
19. W ramach zadań oprogramowanie musi pozwalać na backup:
    1. Wielu lub pojedynczych plików
    2. Wielu lub pojedynczych katalogów
    3. Wielu lub pojedynczych dysków
    4. Wielu lub pojedynczych maszyn (fizycznych i wirtualnych)
    5. Wielu lub pojedynczych baz danych

**Środowiska fizyczne i bazy danych**

1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.
2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.
3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.
4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.
5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.
6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych.
7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.
8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.
9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.
11. Rozwiązanie powinno wspierać odtwarzanie danych w scenaruszach P2P, P2V, V2P, V2V.
12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).
13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.
14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

**Monitoring środowiska oprogramowania**

1. Oprogramowanie musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).
2. Oprogramowanie musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.
3. Oprogramowanie musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
4. Oprogramowanie musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy wirtualizacyjnej.

**Raportowanie**

1. Oprogramowanie raportowania musi umożliwić tworzenie raportów z dostarczonej infrastruktury wirtualnej.
2. Oprogramowanie musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach.
3. Oprogramowanie musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.
4. Oprogramowanie musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.
5. Oprogramowanie musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.

**Odzyskiwanie**

1. Oprogramowanie dostarcza narzędzie do zaplanowania i zautomatyzowania całego procesu odtwarzania awaryjnego systemów.
2. Możliwość tworzenia własnych scenariuszy odtworzeniowych i testowych.
3. Pełna automatyzacja testów Disaster Recovery **dla środowiska Vmware**

**Anty-ransomware i bezpieczeństwo**

1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").
2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System
3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.
4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.
5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczanym urządzeniu.

**Wydajność**

1. Architektura systemu backupowego umożliwi wykonywanie backupów maszyn wirtualnych i aplikacji bez znaczącego obciążania podsystemów (CPU, RAM) środowiska wirtualnego Zamawiającego

Uszczegółowienie: Zamawiający dopuszcza obciążenie środowiska wirtualnego Zamawiającego przez proces backupu na poziomie:

* 1. CPU – obciążenie nie większe niż 10% mocy każdego serwera ESX
  2. RAM – wykorzystanie nie większe niż 6 GB rozmiaru pamięci RAM każdego serwera ESX

1. System backupowy umożliwi wykonanie odtworzenia pojedynczego pliku o rozmiarze ~1 GB (±5%) z kopii wzorcowej maszyny wirtualnej o rozmiarze ~20 GB do innej maszyny wirtualnej w czasie nie dłuższym niż 1 minuta.
2. System backupowy umożliwi wykonanie odtworzenia pojedynczej wzorcowej maszyny wirtualnej o rozmiarze ~20 GB (±5%) pod inną nazwą i do innego datastora w czasie nie dłuższym niż 20 minut.

**Uwagi**

W przypadku konieczności zakupu innego oprogramowania (np. Windows Serwer) lub licencji na usługi/produkty Wykonawca uwzględni je w swoich kosztach. W przypadku licencji czasowych wymagany jest okres 3 lat od zakończenia dostawy, bez kosztowego korzystania z pełnej funkcjonalności.

* + - 1. **Szkolenia 6 osób**

**Warunki szkolenia**

Ilość osób do szkolenia: 6 (2 grupy po 3 osoby).

Każda z grup ma odbywać szkolenie w innym terminie (rozłącznym)

Szkolenie powinno trwać min 6h, w tym:

min. 2 godziny teorii

min. 3 godzin warsztatu

Szkolenie musi odbyć się w ośrodku szkoleniowym znajdującym się na terenie Krakowa

Szkolenie musi być prowadzone w języku polskim

Szkolenie musi być prowadzone przez oficjalnych partnerów, trenerów i dostawców szkoleń, którzy przeszli weryfikację producenta oprogramowania i urządzeń

Szkolenie musi obejmować:

1. Konfigurację urządzeń do przechowywania kopii zapasowych
2. Mechanizmy deduplikacji
3. Mechanizmy szyfrowania
4. Zarządzanie repozytoriami
5. Konfigurację systemu backupowego
6. Wykonywanie backupów
7. Tworzenie planów backupu
8. Wykonywanie odtwarzania (testowe i produkcyjne)
9. Konfiguracja automatycznych odtworzeń
10. Konfigurację powiadomień i raportów

Wykonawca zapewni dla każdego uczestnika wersję elektroniczną materiałów dydaktycznych zawierających streszczenie/omówienie wszystkich zagadnień zawartych w programie szkolenia oraz wykorzystane prezentacje

Wykonawca po zakończeniu szkolenia wystawi uczestnikom dokument/certyfikat potwierdzający odbycie szkolenia wraz z jego zakresem.

* + - 1. **Wdrożenie i wykonanie dokumentacji**

**Wdrożenie**

1. Analiza i wykonanie projektu systemu backup uwzględniającego wymagania Zamawiającego:
   1. Architekturę rozwiązania (szpital posiada 2 serwerownie w 2 różnych lokalizacjach)
   2. Konfiguracje sprzętową urządzeń
   3. Sposób podłączenia oferowanej infrastruktury do infrastruktury Zamawiającego
   4. Adresację sieciową
   5. Konfigurację infrastruktury systemu backupowego
   6. Konfigurację systemu backupowego, w szczególności konfiguracja:
      1. Repozytoriów
      2. Zadań backupowych
      3. Zadań weryfikacyjnych
      4. Replikacji
      5. Monitoringu
2. Dostawa i instalacja
   1. Dostawa urządzeń do lokalizacji Zamawiającego
   2. Montaż dostarczonych urządzeń w szafach rack, w tym zasilanie, LAN
   3. Instalacja i inicjacja licencji (o ile wymagane) na urządzeniach
   4. Uruchomienie dostarczonych urządzeń
3. Konfiguracja
   1. Instalacja na urządzeniach najnowszych wersji oprogramowania wbudowanego
   2. Konfiguracja urządzeń
   3. Instalacja najnowszych aktualizacji systemu backupowego
   4. Konfiguracja infrastruktury systemu backupowego z uwzględnieniem wymagań na system backupowy
   5. Integracja ze środowiskiem Zamawiającego
   6. Konfigurację systemu backupowego (instancja produkcyjna i ewentualnie testowa) do backupu środowiska Zamawiającego i zgodnie z wymaganiami Zamawiającego, w szczególności konfiguracja:
      1. Repozytoriów
      2. Zadań backupowych dla maszyn i aplikacji
      3. Zadań weryfikacyjnych
      4. Replikacji
      5. Monitoringu
4. Instruktaże na środowisku produkcyjnym:

W siedzibie zamawiającego wykonane przez pracownika Wykonawcy obejmujące:

* 1. Tworzenie zadań i planów,
  2. Podłączanie nowych maszyn,
  3. Testowe odtworzenia
  4. Weryfikacja stanu wykonywania backupów

Czas trwania 3 g (grupa) 2 grupy po 3 osoby.  
 Testy:

* 1. Uruchamianie, zatrzymywanie systemu backupowego
  2. Uruchamianie, zatrzymywanie elementów infrastruktury systemu backupowego
  3. Wykonywanie backupów maszyn wirtualnych i aplikacji
  4. Weryfikacja poprawności działania replikacji
  5. Wykonywanie weryfikacji poprawności wykonania backupów
  6. Wykonywanie odtworzenia kopii zapasowych maszyn wirtualnych i aplikacji
  7. Weryfikacja działania alertów
  8. Weryfikacja czasu wykonania backupu inicjalnego środowiska wirtualnego Zamawiającego i zajętości repozytorium po wykonaniu backupu inicjalnego
  9. Weryfikacja czasu wykonania cyklu backupów codziennych środowiska wirtualnego Zamawiającego i zajętości repozytorium po wykonaniu cyklu backupów dziennych
  10. Weryfikacja czasu wykonania odtworzenia pojedynczego pliku o rozmiarze ~1 GB z kopii wzorcowej maszyny wirtualnej
  11. Weryfikacja czasu wykonania odtworzenia pojedynczej wzorcowej maszyny wirtualnej o rozmiarze ~20 GB

**Dokumentacja**

Dokumentacja ma być sporządzona w języku polskim, wykonana w formie elektronicznej, edytowalnej (np. docx).

Dokumentacja powykonawcza

* + - 1. Schemat infrastruktury systemu backupowego wraz z opisem
      2. Zasady licencjonowania dostarczonych elementów infrastruktury systemu backupowego
      3. Informacje o ograniczeniach technologicznych (np. na ilość procesorów, ilość i rozmiar kości pamięci, liczba dysków, itp.) dostarczonych elementów infrastruktury systemu backupowego
      4. Konfigurację sprzętową i logiczną elementów infrastruktury systemu backupowego obejmującą wszystkie elementy wdrożone, zainstalowane w ramach budowy systemu
      5. Raport z przeprowadzonych testów

**Procedury i Polityki**

**Polityka backupu**

Cele

Dane

Harmonogramy

Metody

Procedury:

Procedury uruchamiania, zatrzymywania systemu backupowego oraz elementów infrastruktury

Procedury konfiguracji i wykonywania backupów

Procedury wykonywania weryfikacji

Procedury wykonywania odtworzenia

Procedury wykonywania odtworzenia systemu backupowego z kopii zapasowej

Procedury uruchamiania systemu backupowego w przypadku awarii dowolnej z dwóch lokalizacji Zamawiającego

Procedury weryfikacji stanu systemu

Procedury dokumentowania pracy systemu backupu

Procedury opisujące standardowe działania administracyjne

Wytyczne (dobre praktyki) dla administratorów

**Plan Odtwarzania Awaryjnego (DRP)**

Zasoby i hierarchia

Procesy krytyczne

RTO dla procesów/systemów

Scenariusze awaryjne

Role

Testowanie i aktualizacja

Wykonawca przekaże zamawiającemu prawa autorskie do wytworzonej dokumentacji.

* + - 1. **Środowisko do przechowywania odseparowanej kopii zapasowej (trzecia kopia)**

Zamawiający wymaga zapewnienia przestrzeni na replikację danych backupowych. Wykonawca musi zaoferować jedną z poniżej opisanych przez Zamawiającego opcji i wycenić ją w formularzu cenowym.

**Parametr oceniany.**

- **opcja 1** - rozwiązanie oparte na chmurze, zgodnie z wymaganiami Zamawiającego- 0 pkt.

- **opcja 2** – dostawa sprzętu i oprogramowania maksymalnie - 40 pkt:

* 30 pkt - za dostawę i integrację urządzenia spełniającego wymagania Zamawiającego
* 40 pkt - za dostawę i integrację urządzenia spełniającego wymagania Zamawiającego oraz dodatkowych funkcji rozwiązania spełniających wymagania Zamawiającego

**Opcja nr 1.**

Rozwiązanie oparte na chmurze.

Wykonawca poniesie wszelkie koszty zapewnienia odpowiedniego miejsca na dane oraz transferu do chmury jak i z chmury do siedziby zamawiającego z uwzględnieniem odtworzeń testowych i ew. produkcyjnych w okresie gwarancji (3 lata).

Wymagania:

|  |  |  |
| --- | --- | --- |
|  | **Minimalna** | **Oferowana** |
| Dostępna przestrzeń | Minimum 40 TB\*) |  |
| Transmisja danych do chmury | Min 100Mb/s\* |  |
| Transmisja danych z chmury | Min 1 Gb/s\* |  |
| Bezpieczeństwo | - Szyfrowanie danych w transporcie i podczas przechowywania (at-rest), silne szyfrowanie, np. AES-256.  - WORM  - transmisja poprzez VPN |  |
| Certyfikaty | Dostawca usług posiada certyfikat ISO 2700 lub równoważny |  |

\*) gwarantowana

**Opcja nr 2.**

Wykonawca dostarczy rozwiązanie (urządzenie z oprogramowaniem i licencjami) spełniające wymagania odmiejscowionej kopii zapasowej (należy uwzględnić odmiejscowienie w architekturze systemu). Jeżeli rozwiązanie wymaga zakupu licencji lub jest ograniczone czasowo wykonawca zapewni 3 letni okres bez kosztowego korzystania z pełnej funkcjonalności systemu.

**Wymagania:**

|  |  |  |
| --- | --- | --- |
| **Nazwa wymagania** | **Wymagania minimalne** | **Parametry oferowane** |
| Obudowa | * Obudowa rack rozmiar: 2U |  |
| Przestrzeń dyskowa | Urządzenie musi oferować pojemność minimum 42 TB netto po RAID 6  W pojemność Urządzenia nie może wliczać się przestrzeń znajdująca się w chmurze (tzw. Cloud). |  |
| Procesor | Procesor: min. 8 rdzeni, min. 16 wątków. Minimalna częstotliwość bazowa procesora 2.6GHz |  |
| Pamięć RAM | Pamięć RAM: 32GB |  |
| Interfejsy | Min. 2szt. Ethernet 1 Gb, Dual SFP28 |  |
| Dyski systemowe | Osobne dyski SSD M.2 nVME działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego |  |
| Zasilanie | Urządzenie musi posiadać redundantne zasilanie |  |
| Gwarancja | Gwarancja NBD on-premise obowiązująca przez min. 36 miesięcy |  |
| Data produkcji | Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2025r. |  |
| Integracja z systemami backup | Urządzenie musi współpracować z oprogramowaniem do zarządzania kopiami bezpieczeństwa dostarczonymi w tym postępowaniu. |  |
| Dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. |  |
| Warunki gwarancji | Zachowanie dysków (zatrzymanie uszkodzonych nośników w przypadku ich awarii) |  |
| Dodatkowe funkcje oprogramowania | Urządzenie służące do odmiejscowionej kopii skonfigurowane w technologii „air-gap”. | TAK/NIE |

**Pakiet nr 4**

**System do zarządzania zasobami IT w Szpitalu Spec. im. J. Dietla w Krakowie**

**1. Przedmiot zamówienia**

Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja systemu do zarządzania zasobami IT w Szpitalu Specjalistycznym im. J. Dietla w Krakowie wraz   
z przeprowadzeniem szkoleń dla pracowników Sekcji Informatyki oraz dostarczeniem dokumentacji powdrożeniowej.

**2. Cel zamówienia**

Celem wdrożenia systemu jest zapewnienie centralnego, bezpiecznego i efektywnego systemu zarządzania infrastrukturą IT Zamawiającego, obejmującego sprzęt, oprogramowanie, sieć oraz bezpieczeństwo urządzeń końcowych.

**3. Realizacja przedmiotu zamówienia :**

W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany będzie do realizacji niżej wymienionych zadań :

* Dostarczenie licencji oprogramowania oferowanego przez Wykonawcę.
* Zapewnienie usługi asysty technicznej dot. udzielonych licencji na okres min. 3 miesięcy
* Instalację i wstępną konfigurację dostarczonego systemu na serwerze dostarczonym przez wykonawcę (działanie ma nastąpić przy ścisłej współpracy z zamawiającym)
* Wykonawca przeprowadzi konfigurację systemu zgodnie z wymaganiami Zamawiającego, w tym konfigurację ról i uprawnień użytkowników
* Przeprowadzenie szkolenia z dostarczonego rozwiązania w zakresie implementacji, konfiguracji i obsługi dla sześciu pracowników Sekcji Informatyki wskazanych przez Zamawiającego. Szkolenie odbędzie się poza siedzibą Zamawiającego z podziałem na dwie grupy po 3 osoby przez dwa dni robocze. Koszt organizacji szkolenia, w całości, pokrywa Wykonawca.
* Przygotowanie instrukcji w zakresie konfiguracji i obsługi dla użytkowników systemu(administratorów).
* Wykonanie dokumentacji powykonawczej w wersji elektronicznej PDF lub DOCx obejmującej najważniejsze informacje?
* Wykonawca zapewni usuwanie błędów oraz wsparcie w rozwiązywaniu problemów związanych z funkcjonowaniem systemu przez okres. min 12 miesięcy od wdrożenia

**4. Wymagania ogólne**

* Licencja oprogramowania min. na 3 lata
* Interfejs użytkownika dostępny w języku polskim
* System musi posiadać architekturę typu Klient-Serwer z dostępem dla użytkownika poprzez przeglądarkę internetową, w szczególności EDGE, Chrome, FireFox, Opera, Safari (wersja przeglądarki nie starsza niż 12 miesięcy).
* System umożliwia pracę równoległą dla 6 użytkowników
* System ma możliwość pracy w systemie operacyjnym Windows (co najmniej Windows 7).
* System musi umożliwiać instalację agenta na serwerach fizycznych i wirtualnych   
  z zainstalowanym i użytkowanym przez Zamawiającego systemem operacyjnym   
  w wersji Windows Server 2003 i wyższej w ilości 50 sztuk.
* System musi umożliwiać instalację agentów na komputerach z użytkowanym przez

Zamawiającego systemem Windows 7 i wyższej w ilości 430 sztuk.

* System musi działać w sieciach o adresacji IPv4.
* System musi spełniać wymogi bezpieczeństwa danych, w tym zgodność z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („RODO”) i innymi przepisami dotyczącymi ochrony danych osobowych.
* Dostęp do systemu możliwy przez logowanie za pomącą uwierzytelnienia dwuskładnikowego.
* Wszystkie funkcjonalności systemu powinny być dostępne w momencie instalacji oprogramowania.
* Dostęp do systemu jest zapewniony za pośrednictwem konsoli webowej bez konieczności instalacji dodatkowych komponentów.
* System działa agentowo.
* System ma możliwość instalacji wersji 64bit.
* System obsługuje bazy danych Postgres oraz MS SQL jako instancje do przechowywania danych.
* System posiada wbudowane funkcjonalności wykonywania backupu bazy danych, odtworzenia bazy danych, zmiany bazy danych.
* System pozwala na podłączenie certyfikatu w formie .PFX(PKCS12).
* System posiada interfejs programowania aplikacji API pozwalający na integrację z innymi systemami.
* System pozwala na wysyłanie powiadomień SMS w zakresie alertów dotyczących zinwentaryzowanego sprzętu.
* System posiada funkcje Geofencing oraz Conditional Exchange Access.

**5. Wymagane funkcjonalności systemu**

* System musi umożliwiać zarządzanie co najmniej:

- 430 stacjami roboczymi,

- 30 serwerami (fizycznymi i wirtualnymi).

* System musi umożliwiać zarządzanie urządzeniami działającymi pod kontrolą:

- Windows 7 i wyższe,

- Windows Server 2008 i wyższe,

- Linux (Ubuntu 10.04 i wyższe),

- Oracle Linux 6 i wyższe,

- Red Hat Enterprise Linux 8 i wyższe,

- CentOS 8,

- Fedora 19,

- Debian 7,

- Linux Mint 13,

- OpenSuse 11,

- Suse enterprise Linux 11,

- Android (wersja 6.0 i wyższe),

- IOS (wersja 4.0 i wyższe),

- Windows Phone (wersja 8.1 i wyższe),

- chromeOS (wersja 57.0 i wyższe),

- macOS 10.7 i wyższe,

- inne systemy równoważne.

**6. Wymagane funkcjonalności oprogramowania**

6.1 System rozpoznaje stacje robocze w ramach Active Directory oraz Workgroup.

6.2 System umożliwia dodawanie załączników takich jak faktury, gwarancje w dowolnym formacie.

6.3 System umożliwia instalację i deinstalację aplikacji z indywidualnymi ustawieniami dla pojedynczych stacji, określonych grup roboczych, użytkowników lub grup użytkowników.

6.4 System umożliwia tworzenie list aplikacji, które będą mogły być instalowane przez samego użytkownika z poziomu stacji roboczej, tzw. Portal samoobsługowy.

6.5 System posiada wbudowane funkcje zarządzania i wdrażania łat systemowych i ServicePack na stacjach roboczych oraz serwerach, w szczególności rozpoznaje sekwencje instalacji.

6.6 Funkcje wdrażania łat obejmują co najmniej oprogramowanie: systemy operacyjne Windows: Vista, 7, 8, 10, 11, Windows Server 2008, 2012, 2016, 2022, Systemy MacOS (wersja 10.7 i wyższe), Microsoft Office, Google Chrome, Opera, Skype, Mozilla Firefox, Adobe Reader, Adobe Acrobat, Adobe Shockwave Player, Adobe Flash Player, Java, inne

6.7 System posiada możliwość włączenia opcji testowania i zatwierdzania poprawek na wybranej grupie komputerów testowych przed instalacją poprawek w całym środowisku produkcyjnym.

6.8 System posiada wbudowane narzędzia rozpoznawania podatności stacji roboczych na zagrożenia w oparciu o brakujące łaty systemowe.

6.9 Architektura systemu umożliwia zarządzanie stacjami roboczymi w sieci LAN, WAN bezpośrednio z poziomu serwera centralnego.

6.10 System posiada wbudowane narzędzia zarządzania zasobami IT, w szczególności rozpoznaje komponenty sprzętowe oraz oprogramowanie zainstalowane na stacjach roboczych.

6.11 System posiada wbudowane narzędzia zdalnego dostępu (sesji) z wykorzystaniem technologii ActiveX, HTML 5, z możliwością uzyskania potwierdzenia użytkownika oraz ma możliwość włączenia opcji nagrywania tych sesji.

6.12 System umożliwia wdrażanie polityk konfiguracji dla systemów Windows, w szczególności polityk dostępu do interfejsu USB, zużycia energii, konfiguracji drukarek i przeglądarek Internet Explorer, Mozilla Firefox, Google Chrome oraz Microsoft Edge.

6.13 Konfiguracja polityk dostępu do USB umożliwia blokowanie co najmniej poniższych typów urządzeń, a także ma możliwość wykluczania z listy zablokowanych konkretnych urządzeń o danym identyfikatorze urządzenia lub danego dostawcy, a dla dysków przenośnych tych, które są szyfrowane za pomocą rozwiązania BitLocker:

- Mysz, Stacja dysków (takie jak napędy USB, zewnętrzne dyski twarde),

- CD ROM,

- Urządzenia przenośne (takie jak telefony komórkowe, kamery cyfrowe i przenośne odtwarzacze multimedialne),

- Dyskietka,

- Bluetooth,

- Obraz (takie jak kamery USB i skanery),

- Drukarka,

- Modem,

- Urządzenia USB Apple (takie jak iPad, iPhone i iPod, łączące się z programem iTunes).

6.14 System posiada wbudowane narzędzia systemowe umożliwiające zdalne uruchomianie stacji roboczych, zdalne zamykanie stacji roboczych, skanowanie, czyszczenie i defragmentację dysków.

6.15 System posiada rozbudowany system zarządzania użytkownikami z podziałem na administratora, audytora, gościa, menadżera zasobów, menadżera łat, z możliwością dodawania nowych ról z określonymi uprawnieniami.

6.16 System posiada możliwość dodania nowego użytkownika systemu z uwierzytelnianiem lokalnym lub Active Directory wraz z obsługą SSO oraz przy wykorzystaniu autoryzacji SAML

6.17 System posiada możliwość włączenia opcji uwierzytelniania dwuskładnikowego, dzięki któremu dostęp do systemu odbywać się będzie poprzez podanie swojego hasła dostępu (lokalnego lub Active Directory) oraz drugiego składnika w postaci jednorazowego hasła wysyłanego na maila (funkcja OTP) lub tokenu z aplikacji uwierzytelniającej (np. Google Authenticator).

6.18 System posiada możliwość uruchamiania instalatora aplikacji z uprawnieniami dowolnego użytkownika.

6.18.1 System posiada mechanizm dwuskładnikowej autoryzacji dla opcji odinstalowania manualnego agenta.

6.19 System umożliwia dodawanie i rozliczanie licencji aplikacji.

6.20 System umożliwia wykrywanie zakazanego oprogramowania i uruchamia działania naprawcze, w tym automatyczne odinstalowanie niepożądanej aplikacji.

6.21 System posiada możliwość włączenia pomiaru wykorzystania wskazanej aplikacji.

6.22 System posiada możliwość blokowania plików wykonywalnych EXE poprzez reguły oparte na ścieżce aplikacji lub wartości hash.

6.23 System umożliwia uruchamianie zdalnego Menedżera Systemu dla systemu operacyjnego Windows bez potrzeby uruchamiania połączenia zdalnego sesją RDP, który pozwoli na: podgląd i zamykanie uruchomionych procesów na stacji roboczej, podgląd, uruchamianie, zatrzymywanie, zmianę stanu usług na stacji roboczej, uruchamianie zdalnego wiersza poleceń, podgląd, dodawanie i modyfikację rejestru systemowego stacji roboczej, przegląd logów systemowych stacji roboczej, podgląd menedżera urządzeń, podgląd udziałów sieciowych

6.24 System umożliwia generowanie następujących raportów:

6.24.1 Raporty Active Directory w zakresie:

- aktualnie zalogowani użytkownicy,

- często zalogowani użytkownicy,

- rzadko logujący się użytkownicy,

- nieaktywni użytkownicy,

- historia logowania użytkownika na poszczególnych komputerach.

6.24.2 Raporty dotyczące poprawek w zakresie:

* Narażone systemy
* Narażone poprawki
* Obsługiwane poprawki
* Brakujące poprawki czekające na zatwierdzenie
* Systemy wymagające ponownego uruchomienia

6.24.3 Raporty inwentaryzacji

6.24.6.1 Raporty dotyczące sprzętu

* Komputery wg systemu operacyjnego
* Komputery wg producenta
* Komputery wg pamięci
* Komputery wg wykorzystania dysku
* Komputery wg wieku
* Komputery wg typu urządzenia
* Zmapowane dyski logiczne

6.24.6.2 Raporty dotyczące oprogramowania

* Oprogramowanie według producenta
* Ostatnio zainstalowane oprogramowanie
* Niedozwolone oprogramowanie
* Wykorzystanie oprogramowania przez komputer
* Klucze produktu oprogramowania
* Komputery z/bez określonego oprogramowania
* Podsumowanie zasad pomiaru użytkowania oprogramowania
* Oprogramowanie specyficzne dla użytkownika

6.24.6.3 Raporty dotyczące licencji

* Zgodność licencji
* Licencje do odnowienia

6.24.6.4 Raporty dotyczące systemu

* Użytkownicy grupy systemu
* Komputery wg usług

6.24.6.5 Raporty dotyczące gwarancji

* Gwarancja niedługo wygaśnie
* Gwarancja wygasła
* Niezidentyfikowane komputery

6.24.6.6 Raporty bezpieczeństwa

* Szczegóły Antivirus
* Szczegóły Bitlocker
* Szczegóły Firewall

6.24.6.7 Raporty skanowania plików multimedialnych

* Szczegóły pliku wg kategorii
* Szczegóły pliku wg rozszerzenia

6.24.4 Raporty dotyczące USB

* Raport wykorzystania USB

6.25 System umożliwia planowanie raportów i przesyłanie ich w formie pliku PDF, XLSX, CSV na podany adres mailowy.

6.26 System umożliwia tworzenie niestandardowych raportów w oparciu o kryteria dostępne z systemu.

6.27 System umożliwia tworzenie niestandardowych raportów w oparciu o wysyłanie zapytań SQL do bazy danych z poziomu konsoli zarządzającej.

6.28 System pozwala otrzymywać SMSy dotyczące alertów inwentaryzacyjnych.

6.29 System umożliwia kopiowanie plików do folderów, kopiowanie wielu plików i kopiowanie folderów.

6.30 System umożliwia zarządzanie flotą urządzeń mobilnych typu smartfony i tablety z zainstalowanymi systemami operacyjnymi:

* Android 4.0 i wyższe,
* iOS 4 i wyższe,
* Windows Phone 8.1 i wyższe,
* Chrome OS 57.0 i wyższe,
* tvOS 7.0 i wyższe.

6.31 System pozwala na konfiguracje OEM na urządzeniach z systemem Android za pomocą aplikacji OEMConfig.

6.32 System pozwala na zdalne zatwierdzanie rozszerzenia jądra i systemu dla macOS.

6.33 System pozwala zatwierdzać uprawnienia żądane przez aplikacje Mac, konfigurując zasady kontroli preferencji polityki prywatności.

6.34 Aplikacja obsługuje usługę VPN Per-App dla urządzeń Mac.

6.35 System pozwala na konfigurację tras DNS i Forwarding w Always-on VPN dla urządzeń z systemem Android.

6.36 System posiada moduł rozpoznawania i dodawania urządzeń poprzez:

* wdrożenie Over-theAir(OTA),
* ręczne dodawanie urządzeń,
* zbiorcze dodawanie urządzeń z pliku CSV,
* uwierzytelnione dodawanie z jednorazowym kodem i/lub poświadczeniami użytkownika AD

6.37 System posiada moduł zarządzania profilami.

6.38 System umożliwia konfigurację polis / profili - konfiguracja ustawień polis dostępu do zasobów organizacyjnych.

6.39 System umożliwia nakładanie restrykcji – szyfrowanie pamięci wewnętrznej urządzenia, ograniczanie użytkowania kamery, Youtube, przeglądarki Safari, itp.

6.40 System posiada funkcję Geofencing – możliwość ograniczenia korzystania z urządzeń mobilnych do wybranych regionów geograficznych.

6.41 System posiada funkcję Conditional Exchange Access – monitorowanie urządzeń mających dostęp do serwera Exchange.

6.42 System posiada funkcję Organizacyjny dostęp - zapewnia dostęp do organizacyjnych zasobów jak mail, Wi-Fi, VPN.

6.43 System umożliwia tworzenie grup urządzeń - tworzenie logicznych grup urządzeń w oparciu o departamenty, lokalizacje, w celu rozróżnienia urządzeń organizacyjnych od BYOD (Bring Your Own Device) i wdrażania polis, restrykcji i dystrybucji aplikacji do wszystkich urządzeń w grupie.

6.44 System posiada moduł zarządzania zasobami, który wyświetla informacje o urządzeniu: szczegóły sprzętu, certyfikaty, zainstalowane aplikacje.

6.45 System posiada moduł zarządzania aplikacjami pozwalający na: zarządzanie i dystrybucja własnych aplikacji i AppStore, integracja z programem Apple VPP, publikacja aplikacji w katalogu aplikacji dla użytkowników na potrzeby samodzielnej instalacji.

6.46 System posiada moduł zarządzania bezpieczeństwem obejmujący: kod dostępu: Wymuszenie kodu w celu blokowania nieautoryzowanego dostępu, zdalna blokada: W celu uniknięcia niepowołanego użycia utraconego urządzenia, pełne czyszczenie: Usunięcie wszystkich danych z telefonu w celu wycieku danych po kradzieży, organizacyjne czyszczenie: Usunięcie tylko danych organizacyjnych i pozostawienie danych prywatnych - funkcjonalność absolutnie kluczowa w przypadku zarządzania urządzeniami BYOD (Bring Your Own Device) w ramach organizacyjnej floty smartfonów.

6.47 System pozwala na dystrybucję certyfikatów CA na urządzenia z systemem iOS oraz Android, przy użyciu profilu certyfikatu.

6.48 System lokalizuje urządzenia z systemem Windows 10, nawet bez instalowania aplikacji MDM w urządzeniach.

6.49 System pozwala na obsługę trybu Kiosk dla urządzeń z systemem Android, z systemem OS 5.0 lub nowszym.

6.50 System pozwala na wyszukiwanie aplikacji w kiosku według nazwy aplikacji.

6.51 System pozwala na konfiguracje konta Android for Work, które zapewnia zaawansowane funkcje zarządzania aplikacjami i funkcje konfiguracyjne.

6.52 System pozwala na konteneryzację urządzeń z Androidem w wersji 5.0 lub nowszej, używając Android for Work.

6.53 System pozwala na konfiguracje uprawnień i konfiguracje aplikacji za pomocą Android for Work.

6.54 System pozwala na cichą instalację aplikacji Sklepu Play przy użyciu Android for Work

6.55 System pozwala na rejestrację urządzeń mobilnych z systemem Windows 10.

6.56 System pozwala na reset urządzenia nawet po wygaśnięciu poświadczeń AD.

6.57 System pozwala na śledzenie i zabezpieczenie utraconych urządzeń przy użyciu trybu utraconego dla urządzeń z systemem Android oraz IOS.

6.58 System obsługuje protokół Simple Certificate Enrollment Protocol (SCEP) do integracji z urzędem certyfikacji za pomocą SCEP w celu automatyzacji dystrybucji certyfikatów klienta na urządzenia z systemem iOS.

6.59 System pozwala na automatyzację przypisywania użytkowników urządzeniom z funkcją DEP.

6.60 System pozwala na korzystanie z certyfikatu Enterprise CA.

6.61 System pozwala na przesyłanie zbiorcze szczegółów APN, co ułatwia dystrybucję zasad APN.

6.62 System pozwala na wyświetlanie niestandardowych wiadomości i zapewnianie funkcji połączeń na ekranie blokady zagubionego urządzenia itp. na urządzeniach z systemem Android oraz iOS.

6.63 System pozwala na powiadamia Administratorów pocztą, gdy zarządzanie urządzeniem zostało odwołane przez użytkowników.

6.64 System pozwala na obsługę Trybu kiosku dla urządzeń, które nie obsługują Android for Work.

6.65 System pozwala na zmianę nazwy urządzenia podczas przekazywania urządzenia.

6.66 System pozwala na łatwe wdrażanie ustawień konfiguracji Online Exchange dla wszystkich użytkowników organizacji w korzystających z konteneryzacji

6.67 System pozwala na wprowadzenie nazwy punktu dostępowego (APN) dla urządzeń Samsung, aby skonfigurować komunikację opartą na komórkowej transmisji danych na zarządzanych urządzeniach.

6.68 system pozwala na konfigurację systemu Android for Work bez pakietu G Suite.

6.69 System pozwala na integrację z urzędem certyfikacji za pomocą SCEP, aby zautomatyzować dystrybucję certyfikatów klienta na urządzenia z systemem Windows.

6.70 System pozwala na obsługę zdalne ponowne uruchamianie urządzeń z systemem Windows 10.Aplikacja powinna pozwalać na obsługę automatycznego usuwania aplikacji / profili powiązanych po usunięciu urządzenia z grupy

6.71 System pozwala na nawiązanie sesji zdalnej na urządzenia Android oraz IOS.

6.72 System pozwala na obsługę historii lokalizacji. Dzięki temu administratorzy mogą wyświetlać i przechowywać lokalizacje obsługiwane przez urządzenie w określonym przedziale czasu.

6.73 System pozwala na wyszukiwanie urządzeń za pomocą numeru telefonu urządzenia.

6.74 system pozwala na import certyfikatów SSL z rozszerzeniami takimi jak .jks i .keystore.

6.75 System pozwala na dystrybucję certyfikatów CA na urządzenia Windows.

6.76 System pozwala na wsparcie dla zarządzania komputerami przenośnymi z systemem Windows 10, komputerami stacjonarnymi i tabletami Surface Pro.

6.77 System pozwala na wsparcie automatycznej instalacji aplikacji Android z obsługą kiosku, jeśli aplikacje nie są obecne na urządzeniu.

6.78 System pozwala na zarządzanie aplikacją Apple Classroom, na urządzenia z systemem iOS 11 i nowszym.

6.79 System pozwala na obsługę i cichą instalację aplikacji Sklepu Play na wszystkie urządzenia z systemem Android przy użyciu Android for Work.

6.80 System pozwala na obsługę zdalną na urządzeniach z iOS.

6.81 System pozwala na zarządzanie treścią, aby zdalnie dystrybuować dokumenty do zarządzanych urządzeń OTA.

6.82 System pozwala na rejestrację Android Zero Touch, aby zdalnie zarejestrować flotę urządzeń, przy aktywacji urządzenia bez interwencji użytkownika.

6.83 System pozwala na obsługę Windows Azure AD Automatic Enrollment / Bulk Enrollment, aby bezproblemowo zarejestrować wiele laptopów, komputerów stacjonarnych bez interwencji użytkownika

6.84 System pozwala na automatyczną instalację aplikacji, która ma być obsługiwana w trybie Kiosk na urządzeniach z systemem iOS.

6.85 System pozwala na integrację z Microsoft Business Store.

6.86 System pozwala na integrację z wieloma kontami DEP.

6.87 System pozwala na obsługę wstępnie zdefiniowanych podstawowych ustawień aplikacji Windows przy użyciu Konfiguracji aplikacji.

6.88 System pozwala jednym kliknięciem dystrybuować aplikacje, profile i dokumenty do grup / urządzeń.

6.89 System udostępnia aplikacje Home and Photo Booth, pod Kioskiem na urządzeniach z iOS

6.90 System pozwala na zarządzanie aktualizacjami systemu operacyjnego w celu zautomatyzowania i zaplanowania aktualizacji systemu operacyjnego na urządzeniach z systemem iOS i Android.

6.91 System pozwala rejestrować urządzenia za pomocą konta Azure w MDM.

6.92 System umożliwia skonfigurowanie adresu URL strony głównej przeglądarki dla urządzeń z systemem Windows.

6.93 System pozwala przesyłać wewnętrzne aplikacje korporacyjne o rozmiarze do 1 GB

6.94 System pozwala administratorom wybrać strefę czasową do ustawienia na zarządzanych urządzeniach mobilnych.

6.95 System pozwala na obsługę Google Play Protect dla urządzeń z systemem Android.

6.96 System pozwala na zabezpieczenie korporacyjnych danych Offica 365 na niezarządzanych aplikacjach.

6.97 System posiada opcję zarządzania systemami Windows 10 poprzez Modern Management.

6.98 System pozwala instalować aplikacje AppStore w trybie cichym na MacBookach, blokować Apple TV w trybie Kiosk i uruchamiać na żądanie polecenia bezpieczeństwa, takie jak Zdalna blokada i Zdalne czyszczenie.

6.99 System pozwala konfigurować zasady i rozpowszechniać aplikacje na Chromebookach Google, używając MDM.

6.100 System pozwala zablokować urządzenia z systemem Windows 10 w jednej aplikacji, używając trybu Kiosk.

6.101 System pozwala zbiorczo zarejestrować wiele urządzeń z systemem Windows 10, a także ułatwia proces aktywacji urządzenia, korzystając z Azure Enrollment (AutoPilot).

6.102 System pozwala wyświetlić listę użytkowników w MDM i powiązanych z nimi urządzeniach w widoku dedykowanym.

6.103 System w ramach zasad ograniczeń zabezpieczeń pozwala wymuszać na użytkownikach uwierzytelnianie przy użyciu identyfikatora FaceID, aby umożliwić programowi Safari i innym aplikacjom automatyczne uzupełnianie haseł i danych karty kredytowej.

6.104 System w ramach zasad ograniczeń zabezpieczeń pozwala zabronić urządzeniom firmowym wykonywania konfiguracji zbliżeniowych dla innych urządzeń, co uniemożliwia takie ustawienia, jak kopiowanie Wi-Fi na niezatwierdzone urządzenia.

6.105 System pozwala poznać szczegóły dotyczące sesji użytkownika oraz zakończenia aktualnie aktywnych sesji.

6.106 System powinna pozwala na obsługę VPN dla urządzeń z systemem Android, IOS oraz Windows 10.

6.107 System wyświetla podstawowe informacje, takie jak IMEI, IMSI, numer telefonu itp. Dla urządzeń mobilnych

6.108 System umożliwia wybór pomiędzy domyślnym programem uruchamiającym urządzenia a programem uruchamiającym MDM dla Kiosku na urządzeniach z Androidem.

6.109 System umożliwia zdalne ponowne uruchamianie urządzeń za pomocą jednego kliknięcia.

6.110 System pozwala wyświetlać warunki użytkowania odnoszące się do organizacji, w aplikacji ME MDM.

6.111 Aplikacja ma umożliwiać przeglądanie / pobieranie listy Urządzeń Mobilnych kwalifikujących się do programu Apple Free Repair.

6.112 System umożliwia konfigurację ustawień prywatności urządzenia, określenie rodzaju danych, które można gromadzić, poleceń do wykonania na urządzeniu itp.

6.113 System pozwala na obsługę wiele metod tymczasowego wyłączania Kiosku na urządzeniach z Androidem. 6.114 System pozwala na wysyłanie powiadomień bezpośrednio na urządzenia mobilne 6.115 System pozwala na pobieranie informacji o kartach SIM na telefonach z systemem Android wyposażonych w podwójną kartą SIM

6.116 System pozwala na automatyzacje aktualizacji aplikacji będących w sklepie aplikacji

6.117 System posiada zintegrowany moduł do wdrażania systemów operacyjnych, które umożliwia przechwytywanie obrazu systemu operacyjnego a następnie pozwala wdrożyć go na komputerach przenośnych i stacjonarnych

6.118 System umożliwia tworzenie tzw. wzorców (ang. Template) dystrybucji obrazów, które pozwalają na dystrybucję przygotowanego obrazu zgodnie z określonymi zasadami takimi jak:

* Zadania po dystrybucji obrazu (Restart, Zamknięcie systemu),
* Zarządzanie tzw. SID,
* Możliwość nadania nazwy komputera,
* Dodanie komputera do domeny Windows,
* Instalacja dodatkowego oprogramowania.

6.119 System posiada możliwość tworzenia zadań dystrybucji pozwalających na automatyzacje procesu dystrybucji obrazów systemów.

6.120 System posiada możliwość podpięcia przygotowanych wzorców dystrybucji (ang. Deployment Template), pozwalający na dystrybucję obrazu przy użyciu kodu, lub wybieranych systemów z dostępnej listy komputerów.

6.121 System pozwala na Import komputerów z pliku np. CSV

6.122 System wspiera następujące metody dystrybucji obrazów:

Multicast, Unicast oraz pozwala na tworzenie harmonogramu tejże dystrybucji.

6.123 System posiada możliwość przechowywania wcześniej zapisanych obrazów w swoim repozytorium

6.124 System posiada możliwość przechowywania informacji o sterownikach, a także zapewnia ich dystrybucje w obrazach

6.125 System posiada możliwość tworzenia bootowalnych mediów a także ich edycję:

* + PXE
  + ISO
  + USB

6.126 System posiada repozytorium możliwych do zainstalowania aplikacji po procesie dystrybucji obrazu a także posiada możliwość edycji tychże aplikacji

6.127 System posiada możliwość migrowania profili użytkownika podczas dystrybucji obrazów

6.128 System posiada możliwość generowania logów a także wyświetlania listy statusów i wykonanych akcji

6.129 Możliwość zarządzania Hello for Buissnes z poziomu MDMa dla Windowsów

6.130 Integracje Out Of the Box z rozwiązaniami:

- ServiceNow,

- Jira,

- Zendesk,

- Tenable VM, Tenable SC,

- Spootlight,

- Insight VM On-prem

- Log360,

- Splunk