Załącznik do umowy nr

BDG.zp.23.1.112.2019

z dnia …… 2019 r.

Szczegółowy opis przedmiotu Umowy

1. **Wymagania podstawowe, dotyczące Oprogramowania** - ManageEngine Desktop Central Multi-language UEM (licencja bezterminowa dla 5 techników i 900 urządzeń) lub równoważne*, o następującej funkcjonalności:

   1.1. Oprogramowanie ma zapewnić zintegrowane zarządzanie (z jednego miejsca) serwerami, laptopami, stacjami roboczymi, urządzeniami przenośnymi m.in. poprzez: zarządzanie konfiguracją (w tym portami USB), dystrybucję oprogramowania, zarządzanie poprawkami, połączenia zdalne przy rozwiązywaniu problemów użytkowników, zarządzanie zasobami (w tym oprogramowaniem, licencjami). Oprogramowanie musi wykorzystywać funkcjonujący u Zmawiającego System Obsługi Zgłoszeń (ManageEngine ServiceDesk Plus) typu helpdesk (musi się zintegrować) .

   1.2. Oprogramowanie musi umożliwiać jego instalację na systemie operacyjnym co najmniej w wersji Windows Server 2012 R2.

   1.3. Interfejs oprogramowania oraz konfiguracji musi być w języku polskim i w całości dostępny z poziomu przeglądarki internetowej (Internet Explorer w wersji 10 lub nowszej, Mozilla 44 lub nowszej, Chrome 47 lub nowszej).

   1.4. Architektura Oprogramowania musi być oparta o agentów instalowanych na urządzeniach (np.: stacjach roboczych, serwerach, urządzeniach mobilnych typu laptop, smartphone, tablet).

   1.5. Architektura Oprogramowania musi dawać możliwość instalacji serwerów dystrybucyjnych w lokalizacjach zdalnych.

   1.6. Oprogramowanie musi wspierać bazy danych: PostgreSQL oraz MSSQL

   1.7. Oprogramowanie musi mieć możliwość zarządzania stacjami roboczymi z zainstalowanym systemem operacyjnym:

      1.7.1. Windows co najmniej w wersjach: 7, 8, 10, Server 2008, 2012, 2016.

      1.7.2. Linux co najmniej w wersjach: Ubuntu 10.04, Red Hat Enterprise Linux 6, CentOS, Fedora 19, Mandriva 2010, Debian 7, Linux Mint 13, OpenSuSE 11, SuSE Enterprise Linux 11.

      1.7.3. Mac OS w wersjach: 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12.

1.8. Oprogramowanie musi rozpoznawać stacje robocze w ramach co najmniej Active Directory, Workgroup.

1.9. Oprogramowanie musi umożliwiać instalację i deinstalację aplikacji z indywidualnymi ustawieniami dla pojedynczych stacji, określonych grup roboczych, użytkowników lub grup użytkowników.

1.10. Oprogramowanie musi mieć wbudowane funkcje zarządzania i wdrażania łat systemowych i ServicePack na stacjach roboczych oraz serwerach, w szczególności musi rozpoznawać sekwencje instalacji. Funkcje wdrażania łat powinny obejmować co najmniej oprogramowanie:

1.10.1. Systemy operacyjne Windows: 7, 8, 10, Server 2008, 2012, 2016.

1.10.2. Microsoft Office

1.10.3. Google Chrome

1.10.4. Opera

1.10.5. Skype

1.10.6. Mozilla Firefox

1.10.7. Adobe Reader

1.10.8. Adobe Acrobat

1.10.9. Adobe Shockwave Player

1.10.10. Adobe Flash Player

1.10.11. Java

1.10.12. WinRar

1.11. Oprogramowanie musi mieć możliwość włączenia opcji testowania i zatwierdzania poprawek na wybranej grupie komputerów testowych przed instalacją poprawek w całym środowisku produkcyjnym.

1.12. Oprogramowanie musi mieć wbudowane narzędzia rozpoznawania podatności stacji roboczych na zagrożenia w oparciu o brakujące łaty systemowe.

1.13. Oprogramowanie musi umożliwiać zarządzanie stacjami roboczymi w sieci LAN, WAN bezpośrednio z poziomu serwera centralnego jak i za pośrednictwem serwerów sond.

1.14. Oprogramowanie musi mieć wbudowane narzędzia zarządzania zasobami IT, w szczególności musi rozpoznawać komponenty sprzętowe oraz oprogramowanie zainstalowane na stacjach roboczych.

1.15. Oprogramowanie musi posiadać możliwość tworzenia list aplikacji, które będą mogły być otwierane i instalowane przez samego użytkownika z poziomu stacji roboczej.

1.16. Oprogramowanie musi posiadać wbudowane narzędzia zdalnego dostępu (sesji) z wykorzystaniem technologii ActiveX, Java, HTML 5, z możliwością uzyskania potwierdzenia użytkownika oraz mieć możliwość włączenia opcji nagrywania tych sesji.

1.17. Oprogramowanie musi umożliwiać 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.

1.18. Oprogramowanie musi posiadać wbudowane narzędzia systemowe umożliwiające zdalne uruchomianie stacji roboczych, zdalne zamykanie stacji roboczych, skanowanie, czyszczenie i defragmentację dysków.

1.19. Oprogramowanie musi mieć możliwość zarządzania użytkownikami z podziałem na administratora, audytora, gościa, menadżera zasobów, menadżera łat, z możliwością dodawania nowych ról z określonymi uprawnieniami.

1.20. Oprogramowanie powinno mieć możliwość dodania nowego użytkownika z uwierzytelnianiem lokalnym lub Active Directory.

1.21. Oprogramowanie powinno mieć możliwość włączenia opcji uwierzytelniania dwuskładnikowego, dzięki któremu dostęp do oprogramowania 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 kodu z aplikacji Google Authenticator.

1.22. Oprogramowanie musi dawać możliwość uruchamiania instalatora aplikacji z uprawnieniami dowolnego użytkownika.

1.23. Oprogramowanie musi umożliwiać dodawanie i rozliczanie licencji aplikacji.

1.24. Oprogramowanie musi umożliwiać wykrywanie zakazanego oprogramowania i uruchamiać działania naprawcze.

1.25. Oprogramowanie musi posiadać możliwość włączenia pomiaru wykorzystania wskazanej aplikacji.

1.26. Oprogramowanie musi mieć możliwość blokowania plików wykonywalnych EXE poprzez reguły oparte na ścieżce aplikacji lub wartości hash.

1.27. Oprogramowanie powinno umożliwiać generowanie następujących raportów:

1.27.1. aktywności użytkowników,

1.27.1.1. aktualnie zalogowani użytkownicy,

1.27.1.2. często zalogowani użytkownicy, rzadko logujący się użytkownicy,

1.27.1.3. nieaktywni użytkownicy,

1.27.1.4. komputery na których często logują się użytkownicy,

1.27.1.5. komputery na których rzadko logują się użytkownicy,

1.27.1.6. komputery na których nie logują się użytkownicy,

1.27.1.7. historia logowania użytkownika,

1.27.1.8. historia logowania użytkowników na poszczególnych komputerach,

1.27.2. użytkowników kontrolerów domeny,

1.27.3. wykorzystania aplikacji w skali całej organizacji,

1.27.3.1. Przyrostowe: dodanego, usuniętego sprzętu i oprogramowania, zabronionego oprogramowania, oprogramowania bez licencji, nowych komputerów.

1.28. Oprogramowanie powinno umożliwiać przechwytywanie obrazu ustawień stacji roboczej.

1.29. Oprogramowanie powinno umożliwiać korzystanie z szablonów definiujących adres IP, nazwę, członkostwo w domenie, ustawienia zgodnie z konfiguracją dla nowych instalacji.

1.30. Oprogramowanie powinno umożliwiać kopiowanie plików do folderów, kopiowanie wielu plików i kopiowanie folderów.

1.31. Oprogramowanie powinno umożliwiać tworzenie własnych raportów na podstawie wbudowanych kryteriów.

1.32. Oprogramowanie powinno umożliwiać budowanie własnych raportów na podstawie zapytań do bazy danych.

1.33. System musi umożliwiać zarządzanie flotą urządzeń mobilnych typu smartphony i tablety z zainstalowanymi systemami operacyjnymi: Android 2.2 i wyższe, iOS 4 i wyższe, Windows Phone 8 i wyższe.

1.34. System musi posiadać moduł rozpoznawania i dodawania urządzeń:

1.34.1. Wdrożenie Over-the-Air (OTA),

1.34.2. Ręczne dodawanie urządzeń,

1.34.3. Zbiorcze dodawanie urządzeń z pliku CSV,

1.34.4. Uwierzytelnione dodawanie z jednorazowym kodem i/lub poświadczeniami użytkownika AD

1.35. System musi posiadać moduł zarządzania profilami:

1.35.1. Konfiguracja polis / profili - konfiguracja ustawień polis dostępu do zasobów organizacyjnych

1.35.2. Restrykcje – szyfrowanie urządzenia, ograniczanie użytkowania kamery, youtube, przeglądarki Safari, itp.
1.35.3. Organizacyjny dostęp - zapewnia dostęp do organizacyjnych zasobów jak mail, Wi-Fi, VPN
1.35.4. Grupy 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

1.36. System musi posiadać moduł zarządzania zasobami
1.36.1. Pełna informacja o urządzeniu: szczegóły, certyfikaty, zainstalowane aplikacje
1.36.2. Wbudowane, predefiniowane raporty

1.37. System musi posiadać moduł zarządzania aplikacjami
1.37.1. Zarządzanie i dystrybucja własnych aplikacji i AppStore
1.37.2. Integracja z programem Apple VPP
1.37.3. Publikacja aplikacji w katalogu aplikacji dla użytkowników na potrzeby samodzielnej instalacji

1.38. System musi posiadać moduł zarządzania bezpieczeństwem
1.38.1. Kod dostępu: Wymuszenie kodu w celu blokowania nieautoryzowanego dostępu
1.38.2. Zdalna blokada: W celu uniknięcia niepowołanego użycia utraconego urządzenia
1.38.3. Pełne czyszczenie: Usunięcie wszystkich danych z telefonu w celu wycieku danych po kradzieży
1.38.4. 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 smartphonów

1.39. System musi realizować funkcjonalności:
1.39.1. Aplikacja powinna pozwalać na dystrybucję certyfikatów CA na urządzenia z systemem iOS, przy użyciu profilu certyfikatu.
1.39.2. Aplikacja powinna zlokalizować urządzenia z systemem Windows 10, nawet bez instalowania aplikacji MDM w urządzeniach.
1.39.3. Aplikacja powinna pozwalać na obsługę trybu Kiosk dla urządzeń z systemem Core Android, z systemem OS 5.0 lub nowszym.
1.39.4. Aplikacja powinna pozwalać na wyszukiwanie aplikacji w kiosku według nazwy aplikacji lub identyfikatora wiązki.
1.39.5. Aplikacja powinna pozwalać na konfiguracje konta Android for Work, które zapewnia zaawansowane funkcje zarządzania aplikacjami i funkcje konfiguracyjne.
1.39.6. Aplikacja powinna pozwalać na konteneryzację urządzeń z Androidem w wersji 5.0 lub nowszej, używając Androida for Work.
1.39.7. Aplikacja powinna pozwalać na konfiguracje uprawnień i konfiguracje aplikacji za pomocą Android for Work.
1.39.8. Aplikacja powinna pozwalać na cichą instalację aplikacji Sklepu Play przy użyciu Android for Work

1.39.9. Aplikacja powinna pozwalać na rejestrację urządzeń mobilnych z systemem Windows 10 z kompilacją Redstone.
1.39.10. Aplikacja powinna pozwalać reset urządzenia nawet po wygaśnięciu poświadczeń AD.
1.39.11. Aplikacja powinna pozwalać na śledzenie i zabezpieczenie utraconych urządzeń przy użyciu trybu utraconego.
1.39.12. Aplikacja powinna obsługiwać protokoł Simple Certificate Enrollment Protocol (SCEP) do integracji z urzędem certyfikacji za pomocą SCEP w celu automatyzacji dystrybucji certyfikatów klienta na urządzenia z systemem iOS.
1.39.13. Aplikacja powinna pozwalać na dystrybucję certyfikatów CA na urządzenia z systemem Android przy użyciu profilu certyfikatu.
1.39.14. Aplikacja powinna pozwalać na automatyzację przypisywania użytkowników urządzeniom z funkcją DEP.
1.39.15. Aplikacja powinna pozwalać na korzystanie z certyfikatu Enterprise CA.
1.39.16. Aplikacja powinna pozwalać przesyłanie zbiorcze szczegółów APN, co ułatwia dystrybucję zasad APN.
1.39.17. Aplikacja powinna pozwalać wyświetlanie niestandardowych wiadomości i zapewnianie funkcji połączeń na ekranie blokady zagubionego urządzenia itp. Na urządzeniach z Androidem.
1.39.18. Aplikacja powinna pozwalać na powiadamia Administratorów pocztą, gdy zarządzanie urządzeniem zostało odwołane przez użytkowników.
1.39.19. Aplikacja powinna pozwalać na obsługę Trybu kiosku dla urządzeń, które nie obsługują Android for Work.
1.39.20. Aplikacja powinna pozwalać na obsługę zmianę nazwy urządzenia podczas przekazywania urządzenia.
1.39.21. Aplikacja powinna pozwalać na łatwe wdrażanie ustawień konfiguracji Online Exchange dla wszystkich użytkowników organizacji w korzystających z konteneryzacji.
1.39.22. Aplikacja powinna pozwalać na wprowadzenie nazwy punktu dostępowego (APN) dla urządzeń Samsung, aby skonfigurować komunikację opartą na komórkowej transmisji danych na zarządzanych urządzeniach.
1.39.23. Aplikacja powinna pozwalać na konfigurację systemu Android for Work bez pakietu G Suite.
1.39.24. Aplikacja powinna pozwalać na integrację z urzędem certyfikacji za pomocą SCEP, aby zautomatyzować dystrybucję certyfikatów klienta na urządzenia z systemem Windows.
1.39.25. Aplikacja powinna pozwalać na obsługę zdalne ponowne uruchamianie urządzeń z systemem Windows 10.
1.39.26. Aplikacja powinna pozwalać na obsługę i bezproblemową migrację licencji aplikacji na iOS, gdy typ instalacji aplikacji zmienia się, aby nie wymagać identyfikatora Apple ID.
1.39.27. Aplikacja powinna pozwalać na obsługę automatycznego usuwania aplikacji / profili po usunięciu urządzenia z grupy
1.39.28. Aplikacja powinna pozwalać na nawiązanie sesji zdalnej na urządzenia Android.

1.39.29. Aplikacja powinna pozwalać na obsługę historii lokalizacji. Dzięki temu administratorzy mogą wyświetlać i przechowywać lokalizacje obsługiwane przez urządzenie w określonym przedziale czasu.
1.39.30. Aplikacja powinna pozwalać na wyszukiwanie urządzeń za pomocą numeru telefonu urządzenia.
1.39.31. Aplikacja powinna pozwalać na import certyfikatów SSL z rozszerzeniami takimi jak .jks i .keystore.
1.39.32. Aplikacja powinna pozwalać na dystrybucję certyfikatów CA na urządzenia Windows, Aplikacja powinna pozwalać na politykę certyfikatów. Filtr zawartości WWW jest obsługiwany dla wszystkich dostępnych przeglądarek na urządzeniach z systemem iOS.
1.39.33. Aplikacja powinna pozwalać na wsparcie dla zarządzania komputerami przenośnymi z systemem Windows 10, komputerami stacjonarnymi i tabletami Surface Pro.
1.39.34. Aplikacja powinna pozwalać na wsparcie automatycznej instalacji aplikacji Android z obsługą kiosku, jeśli aplikacje nie są obecne na urządzeniu.
1.39.35. Aplikacja powinna pozwalać na zarządzanie aplikacją Apple Classroom, na urządzenia z systemem iOS 11 i nowszym.
1.39.36. Aplikacja powinna pozwalać na obsługę i cichą instalację aplikacji Sklepu Play na wszystkie urządzenia z systemem Android przy użyciu Android for Work.
1.39.37. Aplikacja powinna pozwalać na obsługę zdalną na urządzeniach z iOS.
1.39.38. Aplikacja powinna pozwalać na zarządzanie treścią, aby zdalnie dystrybuować dokumenty do zarządzanych urządzeń OTA.
1.39.39. Aplikacja powinna pozwalać na rejestrację Android Zero Touch, aby zdalnie zarejestrować flotę urządzeń, przy aktywacji urządzenia bez interwencji użytkownika.
1.39.40. Aplikacja powinna pozwalać na obsługę Windows 10 Admin Subsrollment, aby bezproblemowo zarejestrować wiele laptopów, komputerów stacjonarnych i powierzchniowych Windows 10 bez interwencji użytkownika
1.39.41. Aplikacja powinna pozwalać na automatyczną instalację aplikacji, która ma być obsługiwana w trybie Kiosk na urządzeniach z systemem iOS
1.39.42. Aplikacja powinna pozwalać na obsługę integrację z Business Store.
1.39.43. Aplikacja powinna pozwalać na integrację z wieloma kontami DEP.
1.39.44. Aplikacja powinna pozwalać na obsługę wstępne definiowanie podstawowych ustawień aplikacji Windows przy użyciu Konfiguracji aplikacji.
1.39.45. Aplikacja powinna pozwalać na obsługę urządzenia grupujące różne platformy w jedną grupę, co ułatwia powiązanie polityk.
1.39.46. Aplikacja powinna pozwalać jednym kliknięciem dystrybuować aplikacje, profile i dokumenty do grup / urządzeń.
1.39.47. Aplikacja powinna pozwalać skonfigurować zasady dotyczące kodów dostępu dla techników logujących się do serwera MDM.
1.39.48. Aplikacja powinna udostępniać aplikacje Home and Photo Booth, pod Kioskiem na urządzeniach z iOS
1.39.49. Aplikacja powinna pozwalać tworzyć role ze wstępnie zdefiniowanymi uprawnieniami do zarządzania niektórymi zarządzanymi grupami urządzeń.

1.39.50. Aplikacja powinna pozwalać na zarządzanie aktualizacjami systemu operacyjnego w celu zautomatyzowania i zaplanowania aktualizacji systemu operacyjnego na urządzeniach z systemem iOS i Android
1.39.51. Aplikacja powinna pozwalać na obsługę integrację z produktem Business Store.
1.39.52. Aplikacja powinna pozwalać na rejestrować urządzenia za pomocą konta Azure w MDM Cloud.
1.39.53. Aplikacja umożliwia przeglądanie / pobieranie listy urządzeń kwalifikujących się do programu Apple Free Repair.
1.39.54. Aplikacja umożliwia skonfigurowanie adresu URL strony głównej przeglądarki dla urządzeń z systemem Windows.
1.39.55. Aplikacja powinna pozwalać na przesyłać wewnętrzne aplikacje korporacyjne o rozmiarze do 1,5 GB
1.39.56. Aplikacja pozwala tworzyć role, umożliwiając technikom zdalne sterowanie urządzeniami przenośnymi
1.39.57. Administratorzy mogą wybrać strefę czasową do ustawienia na zarządzanych urządzeniach mobilnych
1.39.58. Aplikacja powinna pozwalać na obsługę Google Play Protect dla urządzeń z systemem Android.
1.39.59. Aplikacja wprowadza nowoczesne zarządzanie urządzeniami Mac i Apple TV. pozwala instalować aplikacje Mac Store w trybie cichym na MacBookach, blokować Apple TV w trybie Kiosk i uruchamiać na żądanie polecenia bezpieczeństwa, takie jak Zdalna blokada i Zdalne czyszczenie.
1.39.60. Aplikacja pozwala konfigurować zasady i rozpowszechniać aplikacje na Chromebookach Google, używając MDM.
1.39.61. Aplikacja pozwala zablokować urządzenia z systemem Windows 10 w jednej aplikacji, używając trybu Kiosk.
1.39.62. Aplikacja pozwala zbiorczo zarejestrować wiele urządzeń z systemem Windows 10, a także ułatwić proces aktywacji urządzenia, korzystając z rejestracji Windows Azure / AutoPilot.
1.39.63. Aplikacja pozwala wyświetlić listę użytkowników w MDM i powiązanych z nimi urządzeniach w widoku dedykowanym.
1.39.64. Aplikacja 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.
1.39.65. Aplikacja 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.
1.39.66. Aplikacja pozwala poznać szczegóły dotyczące sesji użytkownika oraz zakończenia aktualnie aktywnych sesji.
1.39.67. Aplikacja powinna pozwalać na obsługę także VPN dla urządzeń z systemem Android.
1.39.68. Aplikacja wyświetla podstawowe informacje, takie jak IMEI, IMSI, numer telefonu itp., Dla laptopów Windows i Surface Pros.

1.39.69. Aplikacja umożliwia wybór pomiędzy domyślnym programem uruchamiającym urządzenia a programem uruchamiającym MDM dla Kiosku na urządzeniach z Androidem.
1.39.70. Aplikacja umożliwia skonfigurowanie ustawień bezpieczeństwa serwera w celu zapewnienia bezpiecznego zarządzania urządzeniami.
1.39.71. Aplikacja powinna pozwalać na obsługę uwierzytelnianie dwuskładnikowe dla logowania technika.
1.39.72. Aplikacja umożliwia zdalne ponowne uruchamianie urządzeń za pomocą jednego kliknięcia.
1.39.73. Aplikacja pozwala wyświetlać warunki użytkowania odnoszące się do organizacji, w aplikacji ME MDM.
1.39.74. Aplikacja umożliwia konfigurację ustawień prywatności urządzenia, określenie rodzaju danych, które można gromadzić, poleceń do wykonania na urządzeniu itp.
1.39.75. Aplikacja powinna pozwalać na obsługę wiele metod tymczasowego wyłączania Kiosku na urządzeniach z Androidem.

1.40. Aplikacja powinna posiadać zintegrowany moduł do wdrażania systemów operacyjnych, które umożliwia przechwytywanie obrazu systemu operacyjnego a następnie pozwala wdrożyć go na komputerach przenośnych i stacjonarnych
1.40.1. Aplikacja powinna umożliwiać tworzenie tzw. wzorców (ang. Template) dystrybucji obrazów, które pozwalają na dystrybucję przygotowanego obrazu zgodnie z określonymi zasadami takimi jak:
1.40.1.1. Zadania po dystrybucji obrazu /Restart, Zamknięcie systemu
1.40.1.2. Zarządzanie tzw. SID
1.40.1.3. Możliwość nadania nazwy komputera
1.40.1.4. Dodanie komputera do domeny Windows
1.40.1.5. Instalacja dodatkowego oprogramowania
1.40.2. Aplikacja powinna posiadać możliwość tworzenia zadań dystrybucji pozwalających na automatyzacje procesu dystrybucji obrazów systemów oraz powinna posiadać możliwość podpięcia przygotowanych wzorców dystrybucji (ang. Deployment Template), pozwalający na dystrybucję obrazu przy użyciu kodu, lub wybieranych systemów z dostępnej listy komputerów.
1.40.3. Import komputerów powinien być możliwy z pliku np. CSV
1.40.4. Aplikacja powinna wspierać następujące metody dystrybucji obrazów:
1.40.5. Multicast, Unicast oraz powinna pozwalać na tworzenie harmonogramu tejże dystrybucji.
1.40.6. Aplikacja powinna posiadać możliwość przechowywania wcześniej zapisanych obrazów w swoim repozytorium
1.40.7. Aplikacja powinna posiadać możliwość przechowywania informacji o sterownikach, a także zapewniać ich dystrybucje w obrazach
1.40.8. Aplikacja powinna posiadać możliwość tworzenia boot'owalnych mediów a także ich edycję: PXE, ISO, USB
1.40.9. Aplikacja powinna posiadać repozytorium możliwych do zainstalowania aplikacja po procesie dystrybucji obrazu a także musi posiadać możliwość edycji tychże aplikacji

1.40.10. Aplikacja powinna posiadać możliwość generowania logów a także wyświetlać listę statusów i wykonanych akcji.

2. Wymagania dodatkowe

2.1. Wykonawca dostarczy i wdroży Oprogramowanie.

2.2. Oprogramowanie musi się zintegrować z funkcjonującym u Zamawiającego Systemem Obsługi Zgłoszeń (ManageEngine ServiceDesk Plus).

2.3. Funkcjonujący u Zamawiającego System Obsługi Zgłoszeń kontaktuje się ze stacjami roboczymi za pomocą agentów umieszczonych na tych stacjach w celu odczytywania informacji o zasobach. Integracja powinna polegać m.in. na zastąpieniu używanego obecnie agenta, agentem Oprogramowania bez utraty posiadanej obecnie funkcjonalności systemu ManageEngine ServiceDesk+ (wymagany jest jeden agent do obsługi Oprogramowania i funkcjonującego u Zamawiającego Systemu Obsługi Zgłoszeń).

2.4. Integracja Oprogramowania z funkcjonującym u Zamawiającego System Obsługi Zgłoszeń musi zapewniać minimum wykonywanie poniższych zadań z poziomu istniejącego Systemu Obsługi Zgłoszeń bez potrzeby osobnego logowania się serwisanta do Oprogramowania:

2.4.1. czytanie danych zasobów ze stacji roboczych, w tym informacje o sprzęcie i zainstalowanym oprogramowaniu i przesyłanie oraz aktualizacje tych danych do systemu obsługi zgłoszeń,

2.4.2. zdalną instalację oprogramowania na stacjach roboczych,

2.4.3. połączenia zdalne do stacji roboczych,

2.4.4. uruchamianie zdalnego czatu z użytkownikiem stacji roboczej,

2.4.5. wykonywanie zadań aktualizacji systemów operacyjnych i aplikacji firm trzecich na stacjach roboczych.

2.5. Oprogramowanie powinno zapewniać wysyłanie w czasie rzeczywistym alarmów o zmianach sprzętowych i oprogramowania na stacjach roboczych, tzw. alarmów inwentaryzacyjnych, alarmy te powinny być przesyłane do funkcjonującego u Zamawiającego Systemem Obsługi Zgłoszeń jako zgłoszenia.

2.6. Oprogramowanie musi mieć możliwość ustawiania alertów w sytuacjach kiedy stacja robocza nie zgłasza się do serwera przez określony wcześniej czas – funkcja ta ma za zadanie pomóc administratorom zareagować na możliwość nieposiadania przez stację roboczą aktualnych polityk/konfiguracji do niej przypisanych.

2.7. Oprogramowanie musi zapewniać skanowanie urządzeń (na których jest zainstalowany agent) wg określanych przez administratora harmonogramów.

2.8. Oprogramowanie musi zapewniać cykliczną weryfikację urządzeń w organizacji pod kątem zgodności z przypisanymi politykami bezpieczeństwa.

2.9. Oprogramowanie posiada możliwość konfiguracji ograniczania i zapewniania dostępu do portów USB na stacjach roboczych na których jest zainstalowany agent.

2.10. Oprogramowanie powinno zapewniać możliwość określenia wykonywanych czynności przez techników w danym przedziale czasowym, a także zapewniać możliwość określenia kto (serwisant) do jakich modułów programu oraz do jakich zasobów ma dostęp.

2.11. Oprogramowanie musi zapewniać możliwość zarządzania, monitorowania i audytu administratorskiego dostępu do systemów i aplikacji obsługujących wybrane kategorie danych (np. dane osobowe).

3. Wdrożenie oprogramowania

3.1. Wykonawca dostarczy, zainstaluje oraz uruchomi Oprogramowanie w siedzibie Zamawiającego na własny koszt na platformie sprzętowo – systemowej dostarczonej przez Zamawiającego o następujących parametrach:

3.1.1. Windows Server 2012 R2

3.1.2. procesor 4 rdzeniowy 2. 0 GHz,

3.1.3. pamięć RAM 8GB,

3.1.4. miejsce na dysku HDD: 50GB.

3.2. Wdrożenie będzie przeprowadzone w dni robocze w godzinach 8.15-16.15.

3.3. Wykonawca dokona integracji Oprogramowania z funkcjonującym u Zamawiającego Systemem Obsługi Zgłoszeń.

3.4. Prowadzona integracja nie może spowodować zakłócenia pracy urządzeń oraz funkcjonującego u Zamawiającego Systemu Obsługi Zgłoszeń. Dopuszcza się maksymalnie 2 godziną przerwę w działaniu funkcjonującego u Zamawiającego Systemu Obsługi Zgłoszeń w godzinach pracy Zamawiającego. Nie dopuszcza się konieczności wymuszonego restartu stacji roboczych. Zastrzeżenie to nie dotyczy serwera, na którym jest instalowane Oprogramowanie. Zamawiający zastrzega sobie prawo do przeprowadzenia wewnętrznych testów wdrożonego Oprogramowania przed podpisaniem cząstkowego protokołu odbioru dotyczącego wdrożenia.

3.5. Zamawiający nie dopuszcza zdalnej instalacji Oprogramowania spoza siedziby Zamawiającego.

3.6. Wykonawca, po poprawnym wdrożeniu Oprogramowania, poinstruuje administratorów Zamawiającego (do 4 osób) oraz praktycznie przećwiczy z nimi wszystkich funkcjonalności Oprogramowania wykorzystywane przez administratorów, w tym odtwarzanie systemu po katastrofie (disaster recovery). W tym

celu, Zamawiający umożliwi dostęp do wdrożonego Oprogramowania poprzez sieć LAN.

3.7. Wykonawca dostarczy w języku polskim dokumentację powdrożeniową Oprogramowania na płycie DVD lub Pendrive w 2 egzemplarzach, w tym (w formie elektronicznej - pendrive lub płyta DVD) dostarczy instrukcję administratora/ użytkownika (jeżeli producent Oprogramowania przewidział taką instrukcję) oraz procedury odtwarzania Oprogramowania po katastrofie.

3.8. Wykonawca zapewni wsparcie techniczne dla wdrożonego oprogramowania. Wsparcie techniczne będzie realizowane na poniższych warunkach:

3.8.1. pomoc techniczna producenta Oprogramowania,

3.8.2. dostęp do Upgrade, Update i ServicePack,

3.8.3. pomoc techniczna w języku polskim,

3.8.4. dostęp do polskiego portalu pomocy technicznej,

3.8.5. dostęp do polskiej bazy wiedzy,

3.8.6. telefoniczną pomoc techniczną w języku polskim w dniach i godzinach pracy Zamawiającego - pomoc będzie udzielana w ciągu 48 godzin od momentu zgłoszenia przez Zamawiającego problemu z Oprogramowaniem,

3.8.7. mailową pomoc techniczną w języku polskim w dniach i godzinach pracy Zamawiającego - pomoc będzie udzielana w ciągu 48 godzin od momentu zgłoszenia przez Zamawiającego problemu z Oprogramowaniem,

3.8.8. zdalną pomoc techniczną w języku polskim w dniach i godzinach pracy Zamawiającego - pomoc będzie udzielana w ciągu 48 godzin od momentu zgłoszenia przez Zamawiającego problemu z Oprogramowaniem,

3.8.9. obsługa zgłoszeń typu „How to”,

3.8.10. opracowywanie nietypowych raportów w ramach Oprogramowania.

* W przypadku rozwiązania równoważnego Wykonawca zobowiązany jest wypełnić załącznik nr 2a do SIWZ, który zostanie załącznikiem do umowy nr BDG.zp.23.1.112.2019.