Załącznik nr 7 do SWZ

Dostawa sprzętu komputerowego w ramach zadania inwestycyjnego pn.:
"Budowa systemu monitoringu miejskiego"

Szczegółowy opis przedmiotu zamówienia.

1.Komputer Stacjonarny – 3 sztuki

Procesor

Osiągający w testach CPU Benchmark PassMark min. 39 500 punktów na dzień 05.01.2022r.
Procesor musi się znajdować na liście PassMark stanowiącej załącznik do SWZ.
Taktowanie procesora bazowe min. 3,2GHz
Taktowanie procesora w trybie turbo min. 5,2 GHz
Procesor minimum 16 rdzeniowy
Ilość pamięci cache min. 30MB

Chłodzenie procesora

Rodzaj chłodzenia: aktywne, chłodzenie powietrzem
Typ budowy: tower, 12 ciepłowodów
Maksymalny poziom hałasu: 24,7 dB
MTBF: min. 150 000h
TDP: min. 140W
Maksymalny przepływ powietrza: min. 82,5 CFM

Pamięć RAM

Min. 128GB DDR5
Min. 4 gniazda pamięci RAM
Min. taktowanie pamięci 4800 MHz
Opóźnienie pamięci nie większe niż CL40
Pamięć zainstalowana i dostarczona przez producenta komputera.
Zamawiający nie dopuszcza rozbudowy, modyfikacji, czy zmiany komponentu przez Wykonawcę.

Karta Graficzna

Osiągający w testach Video Card Benchmark PassMark min. 26 000 punktów na dzień 05.01.2022r.
Karta graficzna musi się znajdować na liście PassMark stanowiącej załącznik do SWZ.
Pamięć własna karty graficznej min. 24GB GDDR6X
Szerokość magistrali pamięci: min. 384 bit
Liczba procesorów renderujących min. 10496

Dyski – SSD

Pojemność: 2TB
Format: m.2 2280
Typ: PCI-e x4 4.0
Prędkość zapisu: min. 5000 MB/s
Prędkość odczytu: min. 7000 MB/s
Typ kości: TLC lub MLC lub SLC
MTBF: min. 1 500 000h
Dodatkowe technologie:

- Technologia TRIM
- 256-bitowe szyfrowanie danych AES
- Technologia S.M.A.R.T

Odpis i zapis losowy: min. 1 000 000 / 1 000 000 IOPS

Dyski-HDD
Ilość dysków HDD w komputerze: min. 3 sztuki
Pojemność: min. 20 TB
Format: 3,5” SATA III
Prędkość obrotowa min. 7200 obr/min.
MTBF: min. 1 200 000h
Pamięć cache: min. 256MB
Dodatkowe informacje:

- Technologia zapisu CMR
- Usługa producenta dysku odzyskiwania danych w razie awarii

Dyski zainstalowane i dostarczone przez producenta komputera.
Zamawiający nie dopuszcza rozbudowy, modyfikacji, czy zmiany komponentu przez Wykonawcę.

Płyta Główna
porty zew.
Minimalna ilość portów:

- 1x HDMI
- 1x DisplayPort
- 1x RJ45 (LAN) 2,5 Gbps
- 3x USB 3.2 Gen. 1
- 2x USB 3.2 Gen. 2
- 4x USB 2.0
- 2x Audio jack

1x S/PDIF

Porty wew.
6x SATA III (6 Gb/s)
1x M.2 PCIe NVMe 4.0 x4 / SATA
3x M.2 PCIe NVMe 4.0 x4
1x PCIe 5.0 x16
2x PCIe 3.0 x16 (tryb x4)
1x USB 3.2 Gen. 2
1x USB 3.2 Gen. 1
2x USB 2.0
2x Złącze ARGB 3 pin
2x Złącze RGB 4 pin
1x Front Panel Audio
1x Złącze wentylatora CPU 4 pin
4x Złącze wentylatora SYS/CHA
1x Złącze pompy AIO
1x Złącze zasilania 4 pin
1x Złącze zasilania 8 pin
1x Złącze zasilania 24 pin
1x Złącze modułu TPM
2x Thunderbolt 4

Łączność
Sieć przewodowa LAN 10/100/1000/2500 Mbps
Karty sieciowe muszą być zaimplementowane przez producenta komputera lub producenta płyty głównej.

Obudowa
Obudowa Full Tower przeznaczona do pracy komputera w pionie.
Suma wymiarów obudowy (długość, wysokość, szerokość) nie większa niż 1420 mm.
Obsługa 9 kart rozszerzeń PCI/PCIe poziomo, 3 karty rozszerzeń PCI/PCIe pionowo
Posiadająca 3 port USB 3.1 gen. 1 na froncie, 2x Audio (in/out) na froncie obudowy
Obsługa chłodzenia procesora o wysokości do 185mm
Obsługa kart graficznych o długości do 524 mm
Możliwość montażu min. 8 dysków 2,5/3,5", 2 dysków 2,5" oraz 2 zatoki zewnętrzne 5,25"
Zainstalowane 3 wentylatory z możliwością rozbudowy do 11 wentylatorów.

Zasilacz
Moc nie mniejsza niż 1200W
Certyfikat sprawności: 80 PLUS Titanium
Układ PFC: Aktywne
Rodzaj okablowania: modularne
Średnica wentylatora min. 135mm
Zabezpieczenia:

- Przed zbyt wysokim prądem (OCP)
- Przeciwprzeciążeniowe (OPP)
- Termiczne (OTP)
- Przeciwprzepięciowe (OVP)
- Przeciwzwarciowe (SCP)
- Przed zbyt niskim napięciem (UVP)

Okablowanie:

- CPU 4+4 (8) pin - 1 szt.
- CPU 8-pin - 1 szt.
- PCI-E 2.0 6+2 (8) pin - 10 szt.
- MOLEX 4-pin - 8 szt.
- SATA - 16 szt.
- EPS12V 20+4 (24) pin - 1 szt.
- FDD - 2 szt.

Certyfikaty
Deklaracja CE
Deklaracja ROHS

System Operacyjny
Microsoft Windows 10 Professional PL w wersji komercyjnej.
System zainstalowany przez producenta komputera.

Zamawiający dopuszcza rozwiązanie równoważne:
System zainstalowany przez producenta komputera.
Nie wymagający aktywacji za pomocą Internetu lub telefonu.
Zainstalowany system operacyjny, w polskiej wersji językowej.
Dołączony nośnik optyczny (CD/DVD) z instalatorem systemu operacyjnego oraz wszystkimi niezbędnymi do poprawnej pracy zestawu komputerowego sterownikami – parametry techniczne i funkcjonalne systemu.
System operacyjny klasy desktop, 64-bit.
Dostępne dwa rodzaje graficznego interfejsu użytkownika poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji, w tym:
1) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy;

2) dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.
Interfejsy użytkownika dostępne w wielu językach do wyboru, w tym:
1) polskim;
2) angielskim.
Zlokalizowane w języku polskim, co najmniej następujące elementy:
1) menu;
2) odtwarzacz multimediów;
3) pomoc;
4) komunikaty systemowe.
Wbudowany system pomocy w języku polskim.
Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim.
Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego.
Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.
Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne.
Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.
Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych.
Zintegrowana z systemem operacyjnym konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.
Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).
Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.
Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.
Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.
Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.
Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie.
Możliwość pracy systemu w trybie ochrony kont użytkowników.
Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa /instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów, w tym:
1) poziom menu;
2) poziom otwartego okna systemu operacyjnego.
Wbudowany system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.
Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
Obsługa standardu NFC (near field communication).

Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
Mechanizmy logowania do domeny w oparciu o:
1) login i hasło;
2) karty z certyfikatami (smartcard);
3) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
Mechanizmy wieloelementowego uwierzytelniania.
Wsparcie dla uwierzytelniania na bazie Kerberos v. 5.
Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu.
Wsparcie dla algorytmów Suite B (RFC 4869).
Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.
Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.
Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.
Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.
Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.
Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający niezawodność i pozwalający tworzyć kopie zapasowe.
Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
Udostępnianie modemu.
Wbudowane oprogramowanie do tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.
Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).
Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.
Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.
Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w układzie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.

Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinsatalacji systemu.

Bezpieczeństwo i oprogramowanie dodatkowe - w formularzu oferty należy podać pełną nazwę oferowanego oprogramowania

System chroniący przed zagrożeniami, posiadający certyfikaty VB100%, OPSWAT, AVLAB +++, AV Comperative Advance +. Silnik musi umożliwiać co najmniej:

- wykrywanie i blokowania plików ze szkodliwą zawartością, w tym osadzonych/skompresowanych plików, które używają czasie rzeczywistym algorytmów kompresji,
- wykrywanie i usuwanie plików typu rootkit oraz złośliwego oprogramowania, również przy użyciu technik behawioralnych,
- stosowanie kwarantanny,
- wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)
- skanowanie urządzeń USB natychmiast po podłączeniu,
- automatyczne odłączanie zainfekowanej końcówki od sieci,
- skanowanie plików w czasie rzeczywistym, na żądanie, w interwałach czasowych lub poprzez harmonogram, w sposób w pełni konfigurowalny w stosunku do podejmowanych akcji w przypadku wykrycia zagrożenia, z możliwością wykluczenia typu pliku lub lokalizacji.
- Zarządzanie „aktywami" stacji klienckiej, zbierające informacje co najmniej o nazwie komputera, producencie i modelu komputera, przynależności do grupy roboczej/domeny, szczegółach systemu operacyjnego, lokalnych kontach użytkowników, dacie i godzinie uruchomienia i ostatniego restartu komputera, parametrach sprzętowych (proc.,RAM, SN, storage), BIOS, interfejsach sieciowych, dołączonych peryferiach.
- Musi posiadać moduł ochrony IDS/IPS
- Musi posiadać mechanizm wykrywania skanowania portów
- Musi pozwalać na wykluczenie adresów IP oraz PORTów TCP/IP z modułu wykrywania skanowania portów
- Moduł wykrywania ataków DDoS musi posiadać kilka poziomów wrażliwości

Szyfrowanie danych:

- Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.
- Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego.

Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive'y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.

Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.
Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.
Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe

dane użytkownika.
Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.
Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware
Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:

- Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli
- Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory
- Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux
- Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.
- Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich
- Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji

Zarządzanie przez Chmurę:

1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach
2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury
3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur
4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy
5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach
6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń
7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej

Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.
Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.

1. Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer
2. Oprogramowanie klienckie, zarządzane z poziomu serwera.

System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:

- różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie
- funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD
- funkcje regulowania połączeń WiFi i Bluetooth
- funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe
- funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi

- funkcje blokowania dostępu dowolnemu urządzeniu
- możliwość tymczasowego dodania dostępu do urządzenia przez administratora
- zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu
- możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka
- możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora
- możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry
- możliwość używania tylko zaufanych urządzeń sieciowych, w tym urządzeń wskazanych na końcówkach klienckich
- funkcję wirtualnej klawiatury
- możliwość blokowania każdej aplikacji
- możliwość zablokowania aplikacji w oparciu o kategorie
- możliwość dodania własnych aplikacji do listy zablokowanych
- zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze
- dodawanie innych aplikacji
- dodawanie aplikacji w formie portable
- możliwość wyboru pojedynczej aplikacji w konkretnej wersji
- dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB
- kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool
- możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.
- możliwość zablokowania funkcji Printscreen
- funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i OSx
- funkcje monitorowania i kontroli przepływu poufnych informacji
- możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików
- możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj
- możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe
- ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe
- ochrona zawartości schowka systemu
- ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL
- możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych
- ochrona plików zamkniętych w archiwach
- Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem
- możliwość tworzenia profilu DLP dla każdej polityki
- wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania
- ochrona przez wyciekiem plików poprzez programy typu p2p

Monitorowanie zmian w plikach:

- Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.
- Funkcje monitorowania określonych rodzajów plików.
- Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.
- Generator raportów do funkcjonalności monitora zmian w plikach.
- możliwość śledzenia zmian we wszystkich plikach
- możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach
- możliwość definiowana własnych typów plików

Optymalizacja systemu operacyjnego stacji klienckich:

- usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku
- optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem
- możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich
- instruktaż stanowiskowy pracowników Zamawiającego
- dokumentacja techniczna w języku polskim

Wspierane platformy i systemy operacyjne:

1. Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)
2. Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)
3. Mac OS X, Mac OS 10
4. Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat

Platforma do zarządzania dla Android i iOS:

- Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę
- Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.

Zarządzanie użytkownikiem

- Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email
- Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika
- Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi
- Musi posiadać możliwość eksportu danych użytkownika

Zarządzanie urządzeniem

- Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO
- Musi umożliwiać import listy urządzeń z pliku CSV
- Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych
- Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta
- Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał
- Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres
- Musi zawierać podgląd aktualnie zainstalowanych aplikacji
- Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,
- Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł
- Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres

Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:
Wymagania dotyczące technologii:

1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową
2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.

3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:
- Microsoft Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących
5. Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie
6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

7. Portal zarządzający musi umożliwiać:
a) przegląd wybranych danych na podstawie konfigurowalnych widgetów
b) zablokowania możliwości zmiany konfiguracji widgetów
c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.
d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności
e) eksport wszystkich skanów podatności do pliku CSV

2. Monitor –TYP1- 4 sztuk
Rozmiar matrycy min. 28”
Typ matrycy: IPS
Powierzchnia matrycy: Matowa
Rozdzielczość natywna: 3840x2160 UHD 4K
Kontrast statyczny min. 1 000:1
Proporcje: 16:9
Jasność min. 300 cd/m2
Odświeżanie matrycy min. 60Hz
Czas reakcji: nie więcej niż 4ms (GTG)
Poziomy/pionowy kąt widzenia: 178/178 stopni
Porty: 1x audio; 2x HDMI, 1x Displayport
Waga: nie więcej niż 5,9kg
Kabel HDMI w zestawie

3. Monitor –TYP2– 1 sztuka
Rozmiar matrycy min. 27”
Typ matrycy: LED, IPS
Typ ekranu: Płaski
Rozdzielczość ekranu: 3840 x 2160 (UHD 4K)
Format obrazu : 16:9
Częstotliwość odświeżania ekranu: 60 Hz
Odwzorowanie przestrzeni barw: Adobe RGB: 99%, DCI-P3: 90%, sRGB: 100%
Liczba wyświetlanych kolorów:1,07 mld
HDR:HDR 10
Czas reakcji: 5 ms (GTG)
Wbudowany kalibrator: Nie
Technologia synchronizacji: Nie posiada

Technologia ochrony oczu: Redukcja migotania (Flicker free), Filtr światła niebieskiego
Wielkość plamki:0,155 x 0,155 mm
Jasność:300 cd/m²
Kontrast statyczny:1 000:1
Kąt widzenia w poziomie: 178 stopni
Kąt widzenia w pionie: 178 stopni
Złącza:
-HDMI 2.0 - 2 szt.
-DisplayPort 1.4 - 1 szt.
-USB 3.1 Gen. 1 (USB 3.0) - 3 szt.
-USB 3.1 Gen. 1 Type-B (USB 3.0) - 1 szt.
-Mini USB
-USB Typu-C (z DisplayPort i Power Delivery) - 1 szt.
-AC-in (wejście zasilania) - 1 szt.
Głośniki: Nie
Obrotowy ekran (PIVOT): Tak
Regulacja wysokości (Height): Tak
Regulacja kąta pochylenia (Tilt): Tak
Regulacja kąta obrotu (Swivel): Tak
Możliwość montażu na ścianie : VESA
VESA : 100 x 100 mm
Klasa energetyczna:G,G (HDR)
Pobór mocy podczas pracy: 55 W
Pobór mocy podczas spoczynku: 0,5 W