Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA.

Parametry minimalne:

1. Komputer stacjonarny – 1 szt.

1). komputer stacjonarny klasy PC wyprodukowany przez jednego producenta;

2). procesor o wydajności min. 12600 pkt w testach PassMark CPU Benchmark na dzień 22.10.2020r;

3). karta graficzna: zintegrowana w procesorze;

4). procesor osiągający w trybie boost min. 4,3 GHz;

5). pamięć RAM: min. 8GB DDR4 o taktowaniu nie mniej niż 2666 MHz;

Możliwość rozbudowy do 16 GB DDR4 – 1 slot pamięci wolny;

6). obudowa mini tower posiadająca min. 2x USB 3.0, 2x USB 2.0 na przednim panelu;

7). czytnik kart pamięci na panelu przednim;

8). zasilacz o mocy maksymalnej 200 W;

9). dysk systemowy min. 512 GB m.2 PCI NVME;

10). wbudowana nagrywarka DVD±RW DL;

11). porty na panelu tylnym płyty głównej: 2x USB 3.0, 2x USB 2.0, 1x RJ-45, 1x VGA, 1x HDMI, 1x Audio.

Złącza graficzne muszą występować na płycie głównej,

12). płyta główna wyprodukowana oraz zaprojektowana przez producenta zestawu komputerowego, trwale oznaczona jego logiem. Zamawiający nie uzna złączy gniazd karty graficznej jako rozwiązanie równoważne.

13). łączność: Bluetooth 4.2, Wi-Fi 802.11 b/g/n, LAN 10/100/1000 ;

14). oprogramowanie systemowe: Microsoft Windows 10 Professional PL;

15). system musi umożliwiać pełną integrację z pracą domenową w ramach Microsoft Active Directory. Klucz licencyjny trwale zaimplementowany w BIOS płyty głównej przez producenta komputera stacjonarnego.

16). wyposażenie dodatkowe:

a). zestaw klawiatura + mysz.

Klawiatura przewodowa w układzie USB, długość kabla min.2m (dopuszcza się przedłużki).

Mysz przewodowa (scroll), długość kabla min. 2m (dopuszcza się przedłużki).

Gwarancja min. 12 mies.

b). kabel zasilający do komputera.

17). Gwarancja producenta: min. 24 miesięcy w standardzie NBD On-Site.

18). Certyfikaty oraz normy:

- Komputer wyprodukowany zgodnie z normą Energy Star 6.0, deklaracja CE producenta komputera stacjonarnego;

2. Monitor:

1). rozmiar matrycy: minimum 34 cale;

2). rozdzielczość: minimum 3440 x 1440pikseli;

3). czas reakcji: maksimum 5 ms;

4). jasność: minimum 300 cd/m2;

5). złącza: 1xHDMI, 1x HDMI-MHL, 1x Displayport, 1x mDP, 6x USB 3.0, 1x Audio;

6). podstawa z regulowanym kątem pochylenia matrycy;

7). pobór energii (podczas pracy) max 55W;

8). montaż VESA 100 x 100;

9). gwarancja producenta: min. 24 miesiące.

3. Antywirus.

1). Rodzaj i funkcje:

a). przeznaczony do kompleksowej ochrony serwerów i stacji klienckich pracujących pod kontrolą systemów z rodziny Microsoft Windows;

b). aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.

2). Architektura:

a). licencja w postaci subskrypcji czasowej: min. 12 miesięcy;

b). serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer;

c). oprogramowanie klienckie, zarządzane z poziomu serwera.

3). Podstawowa funkcjonalność:

a). 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.

b). 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;
- 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.

4). Zarządzanie i administracja:

a). 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.

b). Zarządzanie przez Chmurę:

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

5). Kontrola urządzeń, aplikacji i DLP:

a). 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.

6). Dodatkowe wymagania:

a). 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 monitorowani;
- 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;

b). 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

7). Wspierane platformy i systemy operacyjne:
- Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit);
- Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit);
- Mac OS X, Mac OS 10;
- Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat.

4. Macierz NAS.

1). typ serwera: RACK;

2). wielkość obudowy: 2U;

3). procesor o wydajności min. 2220 pkt w testach PassMark CPU Benchmark na dzień 22.10.2020r. Procesor osiągający w trybie boost min. 2,3 GHz, czterordzeniowy;

4). pamięć RAM: min. 4 GB z możliwością rozbudowy do 8GB;

5). 2 gniazda pamięci RAM wolne;

6). ilość dysków: obsługa do 8 dysków 3,5”;

7). ilość zainstalowanej pamięci: 8x 4TB dysk HDD o przeznaczeniu do pracy ciągłej w serwerach typu NAS;

8). obsługiwany typ dysków: SSD, HDD;

9). obsługa funkcji hot-swap;

10). architektura sieci: Gigabit Ethernet;

11). ilość portów: RJ-45: minimum 4;

12). pozostałe porty: 1x HDMI, 4x USB 3.0;

13). ilość zainstalowanych wentylatorów: minimum 2.

14). zasilanie: moc zasilacza do 250W;

15). gniazda rozszerzeń: 2x PCIe 2.0 x1;

16). kontroler RAID: wbudowany;

17). poziomy RAID: 0, 1, 5, 6;

18). fizyczny przycisk zasilania i restartu urządzenia;

19). maksymalny poziom hałasu: nie więcej niż 28,5 db(A);

20). oprogramowanie producenta serwera (klient) na następujące systemy:
- Apple Mac OS 10.10 or later;
- Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 or later Linux;
- IBM AIX 7, Solaris 10 or later UNIX;
- Microsoft Windows 7, 8, and 10*;

- Microsoft Windows Server 2008 R2, 2012, 2012 R2 and 2016, 2019.

21). Gwarancja producenta: min. 24 miesiące

5. Wykonawca zapewni kompleksową, pełną konfigurację wg. wskazań zamawiającego, mającą na celu uruchomienie urządzenia wraz z konfiguracją funkcjonalności oprogramowania dodatkowego oferowanego przez producenta sprzętu oraz podłączenie urządzeń zamawiającego do macierzy NAS dostarczonej w ramach postępowania.