**Załącznik 3f do SWZ**

**ZP.271.6.2022**

Program antywirusowy umożliwiający budowanie barier przed falą cyberataków. 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,

• wykrywanie i usuwanie fałszywego oprogramowania bezpieczeństwa (roguewear)

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.

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.

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

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 blokowania dostępu dowolnemu urządzeniu

• 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

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

Moduł oprogramowania 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

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. 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

Backup i przywracanie danych (licencja wieczysta)

- Deduplikacja danych na źródle,

- Backup przyrostowy i różnicowy,

- Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,

- Backup danych lokalnych – plikowy oraz poczty Outlook,

- Backup otwartych plików (VSS),

- Filtr plików oraz folderów,

- Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),

- Wyłączanie komputera po wykonaniu backupu,

- Przywracanie danych do wskazanej lokalizacji,

- Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,

- Wyszukiwanie plików w repozytorium użytkownika,

Ustawienia

- Automatyczne logowanie,

- Zapamiętywanie danych logowania,

- Automatyczne uruchamianie programu przy starcie systemu,

- Ustawianie priorytetu dla procesu backupu,

- Zmiana klucza szyfrującego,

- Ustawienia przepustowości/zajętości pasma,

- Konfiguracja wydajności procesu backupu,

Bezpieczeństwo

- Zastępowanie nazwy pliku GUID-em,

- Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,

- Kompresja danych,

- Transmisja po bezpiecznym protokole TLS,

- Deklaracja klucza szyfrującego dane użytkownika,

- Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,

- Obliczanie sumy kontrolnej,

- Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.

WSPIERANE SYSTEMY OPERACYJNE - opisane szczegółowo w załączniku 3c do SWZ. Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczone w języku polskim, zawarte jest w cenie licencji.