Załącznik Nr 2
do zapytania ofertowego

MINIMALNE PARAMETRY WYMAGANE PRZEZ ZAMAWIAJĄCEGO

I. Specyfikacja sprzętu komputerowego:

1. Komputer przenośny typu notebook z ekranem o wielkości 15,6 cala o rozdzielczości co najmniej 1920x1080 z podświetleniem LED i Anti-Grale, jasność min. 250 nits,.
2. Procesor minimum dwurdzeniowy ze zintegrowaną grafiką, osiągający w teście wydajności PassMark Performance Test lub równoważny co najmniej wynik 6280 punktów wg wyników dostępnych na stronie: http://www.passmark.com/products/pt.htm (Wydruk ze strony www.passmark.com potwierdzający wynik testów PassMark Performance Test).
3. Zainstalowane min. 8 GB pamięci RAM (koniecznie w jednym module).
4. Pamięć masowa – nie mniej niż 512 GB w technologii SSD ze złączem M.2 PCIe.
5. Zintegrowana karta graficzna.
6. Karta dźwiękowa zintegrowana z płytą główną, wbudowane głośniki.
7. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie.
8. Bateria o pojemności co najmniej 30 Whr.
9. W zestawie wymagany dedykowany zasilacz.
10. Czytnik kart pamięci 4in1 (MMC, SD, SDHC, SDCX).
11. BIOS zgodny ze specyfikacją UEFI, wymagana pełna obsługa za pomocą klawiatury i urządzenia wskazującego (wmontowanego na stałe) oraz samego urządzenia wskazującego.
12. Oferowany komputer musi zostać dostarczony z licencją oprogramowania systemu operacyjnego Windows 10 PL 64bit z najnowszą aktualizacją 1909 (Nie dopuszcza się wersji Windows 10 Pro).
13. Wbudowane porty – co najmniej: 1 x HDMI złącze słuchawkowe i mikrofonowe (dopuszcza się złącze współdzielone – combo), co najmniej 2 porty USB 2.0, 1port USB 3,0, 1 port USB typu C.
14. Wbudowany mikrofon z funkcją redukcji szumów i poprawy mowy oraz kamera internetowa HD720.
15. Bezprzewodowa karta sieci Wi-Fi 802.11 b/g/n/ac, Bluetooth.
16. Gwarancja: 24 miesiące.
17. Waga do 1,9 kg.

II. Specyfikacja oprogramowania antywirusowego G Data AntiVirus:

1. Pełne wsparcie dla systemów operacyjnych Windows 7/8/8.1/10.
2. Wsparcie dla 64-bitowych wersji systemów Windows 7/8/8.1/10.
3. Interfejsy programu, pomoce i podręczniki w języku polskim.
4. Pomoc techniczna w języku polskim.
5. Ochrona przed zagrożeniami typu 0-day na poziomie co najmniej 96,6% we wszystkich testach niezależnej organizacji AV-TEST przeprowadzonych w latach 2016 -2018.

Ochrona antywirusowa

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych programów: adware, spyware, scareware, phishing, hacktools itp.
3. Wbudowana technologia do ochrony przed rootkitami wykrywająca aktywne i nieaktywne rootkity.
4. Wbudowany moduł do ochrony przed exploitami.
5. Dedykowany moduł do ochrony przed ransomware.
6. Mechanizm ochrony przed zamaskowanym złośliwym kodem wykorzystujący sieć neuronową opartą o algorytmy adaptacyjne.
7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Dwa niezależne skanery antywirusowe (nie heurystyczne!) z dwoma niezależnymi bazami sygnatur wirusów wykorzystywane przez skaner dostępowy, skaner na żądanie oraz skaner poczty elektronicznej.
9. Możliwość konfiguracji programu do pracy z jednym skanerem antywirusowym albo dwoma skanerami antywirusowymi jednocześnie.
10. Technologia kontroli zachowania aplikacji.
11. Kontrola rejestru i plików autostartu.
12. Sygnalizacja infekcji dźwiękiem.
13. Kontrola autostartu – możliwość opóźnienia uruchamiania aplikacji z autostartu podczas startu systemu.
14. Funkcja skanowania w trybie bezczynności – umożliwiająca pełne skanowanie komputera, uruchamiana i wznawiana automatycznie, podczas gdy komputer nie jest używany. Skanowanie uruchamia się maksymalnie 2 tygodnie po ukończeniu poprzedniego skanowania.
15. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików na żądanie lub według harmonogramu.
16. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
17. Wykrywanie obecności zasilania bateryjnego przed uruchomieniem skanowania.
18. Skanowanie na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym.
19. Możliwość 3-stopniowej regulacji obciążenia generowanego przez program.
20. Możliwość eksportu i importu ustawień programu.
21. Opcja importu ustawień programu umożliwia dodatkowo wybór importowanych funkcji/ustawień.
22. Możliwość zabezpieczenia ustawień programu hasłem.
23. Możliwość określania poziomu obciążenia procesora podczas skanowania na żądanie i według harmonogramu.
24. Możliwość wyłączenia komputera po zaplanowanym skanowaniu jeśli żaden użytkownik nie jest zalogowany.

25. Możliwość skanowania dysków sieciowych i dysków przenośnych.
26. Opcja skanowania dysków przenośnych wywoływana jest automatycznie lub za dodatkowym potwierdzeniem przez użytkownika.
27. Rozpoznawanie i skanowanie wszystkich znanych formatów kompresji.
28. Możliwość definiowania listy plików, folderów i napędów pomijanych przez skaner dostępowy.
29. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
30. Dedykowany moduł ochrony bankowości internetowej, nie bazujący na bazach sygnatur wirusów jak i analizie heurystycznej (heurystyce). Moduł ten współpracuje z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
31. Dodatek do aplikacji MS Outlook umożliwiający podejmowanie działań związanych z ochroną z poziomu programu pocztowego (funkcje dostępne bezpośrednio z programu pocztowego).
32. Skanowanie i oczyszczanie poczty przychodzącej POP3 w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
33. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
34. Możliwość definiowania różnych portów dla POP3, SMTP i IMAP na których ma odbywać się skanowanie.
35. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odebranej wiadomości e-mail oraz tylko do zainfekowanych wiadomości e-mail.
36. Skanowanie ruchu HTTP. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
37. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
38. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
39. Ochrona przed stronami phishingowymi działającymi przy użyciu protokołów HTTP i HTTPS.
40. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe.
42. Aktualizacja dostępna z bezpośrednio Internetu, lub offline – z pliku pobranego zewnętrznie.
43. Obsługa aktualizacji poprzez: eksport baz sygnatur wirusów i późniejszy ich import np. na innym komputerze.
44. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
45. Możliwość określenia częstotliwości aktualizacji w odstępach 1 godzinowych.
46. Program wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego

korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, skaner HTTP).

47. Raportowanie wykrytych zagrożeń i wszystkich przeprowadzonych działań.
48. Kreator nośnika startowego umożliwiający stworzenie podsystemu skanującego komputer bez udziału systemu operacyjnego.
49. Kreator nośnika startowego potrafi nagrać obraz podsystemu skanującego bezpośrednio na nośnik CD/USB, alternatywnie zapisać go na dysku w celu późniejszego wykorzystania.
50. System operacyjny wykorzystywany przez płytę startową umożliwia uaktualnienie sygnatur wirusów przez Internet przed rozpoczęciem skanowania.
51. System operacyjny wykorzystywany przez płytę startową automatycznie wykrywa sieci bezprzewodowe.
52. Wbudowane i ukryte w programie narzędzie diagnostyczne do pomocy technicznej.
53. Interfejs programu informuje o terminie ważności licencji.
54. Program wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
55. Użytkownik ma możliwość podejrzenia numeru rejestracyjnego zastosowanego w programie.

Każdy komputer przenośny powinien mieć:

- założone w systemie lokalne konto administratora i użytkownika,
- system operacyjny powinien być zaktualizowany co najmniej do wersji 1903-OS Build 18362.836 and 1909-OS Build 18363.836,
- zainstalowane oprogramowanie antywirusowe z subskrypcją licencji na 3 lata,
- wszystkie komputery przenośne powinny zostać opisane w protokole dostawy i powinny zawierać: producent i nazwa komputera, nr seryjny, hasło administratora i użytkownika
- każdy komputer powinien być oznaczony naklejką zawierającą logo i nazwę projektu