Załącznik nr 1 do SIWZ

Nr postępowania: BAG.261.14.2020

Szczegółowy opis przedmiotu zamówienia

1. Przedmiot zamówienia – część 1:

Zakup oprogramowania antywirusowego na okres 24 miesięcy

1.1. **Subskrypcje:**

- 350 subskrypcji

2. Wymagania minimalne dla kompleksowej ochrony antywirusowej :

2.1. Wymagania techniczne/systemowe

1. Systemy Operacyjne Komputerów:
   - Windows 10
   - Windows 8.1
   - Windows 8
2. Urządzenia Mobilne:
   - Apple iPhone i tablety iPad (wersja iOS 10 +)
   - Smartfony i tablety z Google Android (wersja Androida 6 +)
3. Systemy operacyjne serwera Windows:
   - Windows Server 2019/2019 Core
   - Windows Server 2016/2016Core
   - Windows Server 2012/2012 R2
   - Windows Server 2008 R2
4. Systemy operacyjne Linux:
   - Ubuntu 14.04 LTS lub wyższy
   - Red Hat Enterprise Linux / CentOS 6.0 lub wyżej
   - Debian 8.0 lub wyższy
5. Środowiska Microsoft Exchange:
   - Exchange Server 2019 z rolą Edge Transport lub Mailbox
   - Exchange Server 2016 z rolą Edge Transport lub Mailbox
6. Środowiska wirtualne:
   - Posiada możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej, do pobrania w formacie OVA
   - VMware vSphere 6.7 update 2a
   - VMware vCenter Server 6.7 update 2a

2.2. Konsola zdalnej konfiguracji/zarządzania:

1. Posiada lokalny serwer administracyjny.
2. Posiada serwer administracyjny w chmurze.
3. Centralna instalacja, konfiguracja i zarządzanie oprogramowaniem do ochrony stacji roboczych i serwerów plikowych Windows, zdalna instalacja na środowiskach wirtualnych z jednego serwera zarządzającego..
4. Posiada funkcje integracji Domeny Active Directory w konsolach.
5. Posiada funkcje synchronizacji serwera administracyjnego z Active Directory.
6. Posiada funkcje uruchomienia zdalnego skanowania wybranych stacji roboczych.
7. Posiada funkcje sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej:
    - aktualnych ustawień programu
    - wersji programu i bazy wirusów
    - wyników skanowania skanera na żądanie
    - zainstalowanych modułów
    - ostatniej aktualizacji
    - zastosowanych polityk
8. Posiada funkcje sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej:
    - adresów IP
    - wersji systemu operacyjnego
9. Posiada funkcje centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
10. Posiada funkcje wysłania polecenia instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
11. Posiada funkcje zmiany konfiguracji na stacjach i serwerach jedynie z centralnej konsoli zarządzającej.
12. Posiada funkcje uruchomienia centralnej konsoli z poziomu przeglądarki internetowej.
13. Posiada funkcje ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv.
14. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum.
15. Posiada funkcje generowania raportu co godzinę.
16. Posiada funkcje dodania etykiety do stacji roboczej.
17. Każdy z rodzajów ochrony musi być rozdzielony w osobnych oknach/zakładkach konfiguracyjnych.
18. Serwer centralnej administracji musi posiadać funkcje przełączenia się miedzy widokiem maszyn fizycznych i urządzeń mobilnych. Tak by wyświetlana była jedynie wskazana grupa urządzeń chronionych.
19. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do dalszego prawidłowego działania programu.
20. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej do dalszej pracy..
21. Posiada funkcje dezinstalacji oprogramowania antywirusowego innych firm.
22. W całym okresie trwania przedmiotu zamówienia użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
23. Posiada aktualizacje serwera administracyjnego bez potrzeby przeinstalowywania go.
24. Tworzenie osobnych polityk dla:

- fizycznych komputerów
- urządzeń przenośnych
- maszyn wirtualnych

25. Posiada funkcje zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
26. Posiada opcje utworzenia konta użytkownika z podziałem na role lub z ustawieniami niestandardowymi.
27. Posiada funkcje przypisywania polityk w zależności od zalogowanego użytkownika domenowego.
28. Posiada funkcje przypisywania polityk w zależności na jakim połączeniu sieciowym użytkownik
    się znajduje.
29. Możliwość integracji z zewnętrznym serwerem Syslog.
30. Posiada uwierzytelnianie dwuskładnikowe.
31. Posiada funkcjonalność, która wspiera powrót do ostatnich działających wersji oprogramowania oraz sygnatur w przypadku instalacji wadliwej aktualizacji.
32. Użytkownik na punkcie końcowym ma możliwość interakcji z oprogramowaniem np. opóźnienia restartu potrzebnego do ukończenia zadań.
33. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy np. security groups.
34. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.
35. Posiada funkcje wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.
36. Kontroli aplikacji, która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów.
37. Kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat.
38. Posiada możliwość integracji z innymi systemami poprzez API takich elementów jak:
    - pakiety
    - sieć
    - kwarantanna
    - integracje
    - raporty
    - konta

2.3. Oprogramowanie Antywirusowe:

1. Kompleksowa ochrona przed zagrożeniami typu:
    - wirus
    - trojan
    - robak
    - adware
    - spyware
    - dialer
    - phishing

- narzędzia hakerskie
- backdoor
- rootkit
- exploit
- ransomware

2. Wsparcie techniczne, interfejs użytkownika oraz dokumentacja dostarczona i świadczona w języku polskim.
3. Opcje skanowania:
   - skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
   - wybór trybu skanowania dla całego dysku, wybranych katalogów lub pojedynczych plików.
   - na żądanie" pojedynczych plików lub katalogów przy pomocy z menu kontekstowego, dysków sieciowych i przenośnych, plików spakowanych i skompresowanych
   - skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu ms outlook, outlook express.
   - skanowanie i oczyszczanie poczty przychodzącej pop3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej.
   - skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
4. Posiada opcje dodawania wykluczeni na podstawie:
   - plik ,folder
   - rozszerzenie
   - proces hash pliku/certyfikatu
   - nazwa zagrożenia
   - wiersz poleceń
5. Powiadomienia z rozwiązania sprawdzającego procesy posiadają :
   - ścieżkę
   - identyfikator procesu nadrzędnego
   - wiersz poleceń, który uruchomił proces
   - przesyłanie za pośrednictwem Syslog
6. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
7. Blokowanie możliwości przeglądania wybranych stron internetowych.
8. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
9. Posiada funkcje definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
10. Program umożliwia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.
11. Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
12. Posiada funkcje zabezpieczenia programu przed deinstalacją za pomocą hasła.
13. Posiada funkcje zdefiniowania w aplikacji danych do pomocy technicznej:
    - adres strony
    - adres e-mail do administratora
    - numer telefonu do administratora
14. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
15. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.

16. Praca programu musi być niezauważalna i nieuciążliwa dla użytkownika.
17. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.
18. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
19. Oprogramowanie stanowiskowe posiada wbudowaną i zintegrowaną funkcję do komunikacji z serwerem administracyjnym, w postaci pojedynczej aplikacji.
20. Posiada opcje odblokowania ustawień programu po wpisaniu hasła.
21. Posiada opcje odblokowania ustawień lokalnych konfiguracji.
22. Wbudowany moduł kontroli urządzeń:
    - posiada funkcje blokowania dostępu do urządzeń
    - podłączenia tylko do odczytu
    - kontrola w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie
23. Posiada opcje dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, z bazy danych urządzeń podłączanych przez użytkowników do komputerów.
24. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak:
    - adresy e-mail
    - piny, Konta bankowe
    - hasła
25. Funkcja Ochrony danych konfigurowana zdalnie przez administratora.
26. Jedna wersja instalacyjna na stacje robocze i serwery plików.
27. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
28. Wbudowany IDS.
29. Posiada funkcje zainstalowania silnika pełnego, lekkiego z sprawdzaniem reputacji plików w chmurze, lub skanowanie przez centralny serwer.
30. Posiada funkcje tworzenia list sieci zaufanych.
31. Posiada możliwość dezaktywacji funkcji zapory sieciowej.
32. Posiada funkcje ochrony systemu operacyjnego bez użycia lokalnego silnika skanującego, jego rolę przejmuje centralny serwer bezpieczeństwa odpowiedzialny za proces skanowania plików.
33. Posiada funkcje wykluczenia aplikacji ze skanowania na podstawie hashu pliku.
34. Posiada opcje ustawienia skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
35. Ochrona przeciwko zagrożeniom typu ransomware.
36. Ochrona proaktywna oparta o maszynowe uczenie.
37. Posiada możliwość wykorzystania rozwiązania typu Sandbox po stronie producenta który pozwala na analizę pliku:
    - plik może zostać wysłany automatycznie lub ręcznie z poziomu konsoli
    - plik nie może przekraczać rozmiaru 50mb
    - posiada funkcje przesłania archiwum zabezpieczonego hasłem
    - posiada funkcje przesłania adresu url
    - w przypadku przesłania wielu plików, posiada możliwość detonacji próbek pojedynczo
38. Posiada wgląd w pamięć Hypervisora.
39. System zarządzania ryzykiem.
40. Ochrona przed Exploitami.
41. Ochrona przed atakami sieciowymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci.

42. Ochrona przed atakami skryptowymi.
43. Pełne Szyfrowanie dysków.
44. Zarządzanie aktualizacjami oprogramowania firm trzecich.
45. Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń dając możliwość:
    - filtrowania zdarzeń
    - blokowania procesów
    - dodawanie procesów do czarnej listy
    - dodawanie procesów do białej listy
    - izolacja hosta, aktualizacja hosta
    - przesłanie pliku do sandbox
    - przesłanie hashu do wyszukiwarki google
    - przesłanie hashu do virustotal
46. Filtrowanie zdarzeń odbywa się na podstawie:
    - ocena zagrożenia
    - data wykrycia
    - status
    - id
    - nazwa punktu końcowego,
    - typ ataku
    - ransomware
    - potencjalnie niechciana aplikacja
    - malware
    - exploit
    - fileless
    - password stealer
    - downloader
47. Wyszukiwanie zdarzeń może odbywać się na podstawie:
    - nazwa alertu
    - ip punktu końcowego
    - hash md5/ sha256
    - nazwa użytkownika
48. Posiada funkcje szybkiego podglądu:
    - otwartych incydentów
    - najczęstszych powiadomień
    - urządzeń na których występują najczęściej problemy.
49. Posiada możliwość zmiany ilości zdarzeń wyświetleniach na jednej stronie.
50. Posiada funkcje wyświetlenia zablokowanych hashy plików.
51. Posiada funkcje dodania własnych hashy MD5 oraz SHA256 oraz Posiada funkcje dodania do tego wpisu własnej notatki.
52. Posiada funkcje importu hashy z pliku CSV.
53. Posiada funkcje filtrowania dodanych hashy na podstawie:
    - typu hashu
    - wartości hash
    - źródło dodania informacje o źródle
    - nazwa pliku

54. Posiada funkcje wykrywania i blokowania ataków typu ransomware oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich.
55. Formaty plików jakie mogą być odzyskane:
    - Cab, cdr, cer, crt, crw, dcr, der, dgn, dll, dng, doc, docm, docx, dwg, dxf, eps, erf, exe, ini, jpe, jpeg, jpg, msg, msi, odb, odc, odp, ods, odt, p12, p7b, p7c, pdf, pef, pem, pfx, png, ppt, pptm, pptx, psd, pst, ptx, py, raf, rtf, srf, srw, wpd, wps, xlk, xls, xlsb, xlsm, xlsx, xml.
56. Posiada możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
57. Dla maszyn z systemem Linux posiada możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym.
58. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
59. Posiada funkcje wskazania do jakiego serwera ochrony maja się łączyć klienci maszyn wirtualnych.
60. Posiada możliwość szyfrowania urządzenia opartego o system android.
61. Posiada możliwość pobrania wersji instalacyjnej ze sklepu iOS oraz Android.
62. Skanowanie aplikacji w trakcie instalacji na urządzeniach z systemem Android.
63. Posiada funkcje wymuszenia szyfrowania urządzenia dla systemu Android.
64. Posiada funkcje blokowania ekranu głównego hasłem.
65. Posiada opcje definiowania połączeń Wi-Fi.
66. Kontrola przeglądarki Safari dla urządzeń z systemem iOS.
67. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
68. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym Posiada funkcje zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w przeciągu ostatnich kilku godzin / dni
69. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz nie możliwych do przeskanowania.
70. Posiada możliwość wykluczenia potencjalnie niechcianych aplikacji z filtrowania antymalware.
71. Posiada funkcje skanowania w poszukiwania malware wewnątrz archiwów.
72. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.
73. Posiada możliwość odpytania serwerów „Realtime Blackhole" List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.
74. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu m.in. alfabetów azjatyckich.
75. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi.
76. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowania maila do konkretnej skrzynki pocztowej.
77. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.

78. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci „taga" do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.

3. Przedmiot zamówienia – część nr 2:

Zakup jednej licencji na aktywację funkcji Data Domain „Retention Lock" - zabezpieczenia zasobów plikowych wraz ze wsparciem technicznym.

3.1. Przedmiot zamówienia odnosi się do posiadanego i wykorzystywanego przez Zamawiającego urządzenia Dell EMC Data Domain DD2200 s/n CKM00182300931

3.2. Funkcja Retention Lock zapewnia blokadę nieautoryzowanej modyfikacji zasobów plikowych, a więc kasowania, modyfikacji i dodawania plików. Oznacza to:

- bezpieczne przechowywanie kopii zapasowych – ochronę przed działaniem szkodliwego oprogramowania, np. ransomware i przypadkową, błędną ingerencją administratorów
- zgodność z normami wewnętrznymi i ustawowymi – ochrona danych archiwalnych przez określony czas.

3.3. Warunki wsparcia technicznego

Wsparcie techniczne powinno być zapewniane przez producenta sprzętu Dell EMC i mieć termin ważności zgodny z aktualnym terminem dla całego urządzenia. Termin może być sprawdzony na odpowiednim portalu producenta.