**Nr sprawy BZP.38.383-7.19**

## Formularz oferty

**Postępowania o udzielenie zamówienia o wartości nie przekraczającej wyrażonej w złotych równowartości kwoty 30 000 euro, na podstawie art. 4 pkt 8 Ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych – procedura udzielenie zamówienia równej lub przekraczającej kwoty 2 000 euro do 30 000 euro, zgodnie z § 22 Regulaminu.**

Część A :

Na wykonanie dostaw/usług/robót budowlanych poniżej 30 000 euro.

L. NAZWA I ADRES ZAMAWIAJACEGO
Samodzielny Publiczny Zakład Opieki Zdrowotnej Wojewódzki Szpital Specjalistyczny Nr 2
Al. Jana Pawła II 7, 44–330 Jastrzębie – Zdrój
REGON: 272790824, NIP: 633-10-45-778, KRS 0000048508

ll. NAZWA PRZEDMIOTU ZAMÓWIENIA:
Zamawiający zaprasza do złożenia oferty na zamówienie pn: **Przedłużenie licencji dla systemu antywirusowego F-SECURE BUSINESS – 360 sztuk.**
Opis przedmiotu zamówienia zawiera załącznik nr 2 do Formularza oferty – Szczegółowy opis przedmiotu zamówienia.

III. TERMIN REALIZACJI ZAMÓWINIA:
Umowa obowiązywać będzie: **od dnia 14.02.2019r. do dnia 13.02.2021r.**

IV. WARUNKI PŁATNOŚĆI
Należność za przedmiot zamówienia płatna będzie w terminie 60 dni od dnia doręczenia faktury do siedziby Zamawiającego. Jako dzień zapłaty przyjmuje się datę obciążenia rachunku bankowego Zamawiającego.

V. INNE WYMAGANIA: (jeżeli dotyczy)

VI. OPIS SPOSOBU ZŁOŻENIA OFERTY:
1. Ofertę na **Formularzu oferty** należy złożyć w terminie do dnia **05.02.2019r. do godz. 10:00:**
• pisemnie, na adres Wojewódzki Szpital Specjalistyczny nr 2, Al. Jana Pawła II 7, 44-330 Jastrzębie - Zdrój, I p, Sekretariat (koperta zaklejona, opisana: Procedura do 30.000 euro BZP.38.383-7.19)- nie otwierać przed 05.02.2019r. godz. 10:00) lub
• faksem z podpisem Wykonawcy (oferta nie podpisana zostanie odrzucona) na numer 032 47 84 549 lub
• w wersji elektronicznej z podpisem Wykonawcy (oferta nie podpisana zostanie odrzucona) e-mail: zp@wss2.pl.

2. Cena w niej podana ma być wyrażona cyfrowo i słownie;
3. Winna być napisana w języku polskim, czytelnie;
4. Winna obejmować całość zamówienia.

VII. OPIS WARUNKÓW UDZIAŁU W POSTĘPOWANIU:
1. Wykonawca winien zapoznać się z opisem przedmiotu zamówienia i wzorem umowy.
2. Wykonawca winien posiadać zdolność techniczną i zawodową umożliwiającą wykonywanie przedmiotu umowy opisanego w pkt II części A Formularza oferty.

VIII. OFERTA MA ZAWIERAĆ NASTĘPUJĄCE DOKUMENTY I ELEMENTY:
1. **Część A i wypełnioną część B** Formularza oferty oraz wypełniony załącznik nr 2 do Formularza oferty.

2. Aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji (kopia potwierdzona za zgodność z oryginałem przez osobę uprawnioną do reprezentowania Wykonawcy).

IX. OPIS SPOSOBU OBLICZENIA CENY W SKŁADANEJ PROPOZYCJI CENOWEJ:
1. W cenie oferty winny zawierać się wszystkie koszty niezbędne do prawidłowego wykonania Zamówienia.
2. W formularzu oferty należy podać cenę oferty: wartość netto i wartość brutto.

X. KRYTERIUM OCENY OFERT:
Kryterium – cena 100%

XI. OSOBAMI WYZNACZONYMI DO KONTAKTU W SPRAWACH:
a) merytorycznych są:
- ze strony Zamawiającego: Szymon Jurkiewicz – Główny Specjalista ds. Informatyki.
b) formalno- prawnych:
- ze strony Zamawiającego: Izabela Sobczak - St. specjalista ds. Zamówień Publicznych.

XII. ZAŁĄCZNIKI:
Załącznik nr 1 – Wzór umowy (lub Istotne postanowienia umowy),
Załącznik nr 2 – Szczegółowy opis przedmiotu zamówienia.

**Część B**

**I NAZWA I ADRES W3YKONAWCY:**

.....
.....
.....
.....

**NIP** ..... **Regon** .....

**e-mail:** .....

**Nazwa banku i numer rachunku bankowego** .....
.....

II. OFERUJĘ WYKONANIE WYŻEJ WYMIENIONEGO PRZEDMIOTU ZAMÓWIENIA ZA CENĘ:
Cena netto: ..... zł /słownie: ...../100
Cena brutto: .....zł /słownie: ...../100
**Cena ogółem:**
**Cena netto:** ..... zł /słownie: ...../100
**Cena brutto:** .....zł /słownie: ...../100

III. OSOBAMI WYZNACZONYMI DO KONTAKTU ZE STRONY WYKONAWCY SĄ:
1. .....
2. .....

IV. OŚWIADCZENIA:
1. Wykonawca oświadcza, że zapoznał się z opisem przedmiotu zamówienia i wzorem umowy i nie wnosi do nich żadnych zastrzeżeń.
2. Wykonawca oświadcza, że wykona przedmiot zamówienia w terminie określonym przez Zamawiającego.
3. Wykonawca oświadcza, iż posiada zdolność techniczną i zawodową umożliwiającą wykonywanie przedmiotu umowy opisanego w pkt II części A Formularza oferty.

V. ZAŁĄCZM DO NINIEJSZEGO FORMULARZA NASTĘPUJĄCE ZAŁĄCZNIKI, STANOWIĄCE INTEGRALNĄ CZĘŚĆ OFERTY:

1. .....
2. .....

Miejscowość ..... dnia .....

.....
Podpis osoby uprawnionej

.....
Pieczęć Wykonawcy

**Załącznik nr 1**

**UMOWY NR ……/2019 - wzór**

Zawarta w dniu ……. 2019 roku w Jastrzębiu - Zdroju pomiędzy:
Samodzielnym Publicznym Zakładem Opieki Zdrowotnej Wojewódzkim Szpitalem Specjalistycznym Nr 2 w Jastrzębiu - Zdroju przy Al. Jana Pawła II 7, zarejestrowanym w Sądzie Rejonowym w Gliwicach Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000048508 nr NIP 6331045778, reprezentowanym przez:
…… – Dyrektora

zwanym dalej „ZAMAWIAJĄCYM"
a
zwanym dalej „WYKONAWCĄ"

**§1**

Umowa zostaje zawarta, w wyniku postępowania BZP.38.383-7.19 o wartości szacunkowej, której wartość nie przekracza wyrażonej w złotych równowartości kwoty 30 000 euro na podstawie obowiązującego u Zamawiającego Regulaminu udzielania zamówień publicznych, stanowiącego załącznik nr 1 do Zarządzenia nr 137/2016 z dnia 02.09.2016 r. Dyrektora Wojewódzkiego Szpitala Specjalistycznego Nr 2 w Jastrzębiu- Zdroju.
Ustawy Prawo Zamówień Publicznych z dnia 29 stycznia 2004 r. na podstawie art. 4 pkt 8 Ustawy PZP nie stosuje się.

**§ 2**
**Przedmiot umowy**

1. Przedmiotem umowy jest: **przedłużenie licencji dla systemu antywirusowego F-SECURE BUSINESS – 360 sztuk.**
2. Szczegółowy opis przedmiotu zamówienia zawarty jest w Załączniku do Umowy Szczegółowy opis przedmiotu zamówienia.
3. Program wykorzystywany będzie do zabezpieczenia w siedzibach Zamawiającego - 360 hostów, w tym 10 maszyn wirtualnych – opartych na 2 fizycznych serwerach Hyper-V.
4. Licencja przedłużona zostanie w ciągu 4 dni kalendarzowych od dnia 14.02.2019r. na okres 24 miesięcy.

**§ 3**

Umowa zostaje zawarta na okres: **od dnia 14.02.2019r. do dnia 18.02.2021r.**

**§ 4**
**Wartość umowy i warunki płatności**

1. Wykonawca zobowiązuje się do przedłużenia licencji, o której mowa w § 2 a Zamawiający do zapłaty umówionej ceny. Za termin przedłużenia licencji uważa się datę przekazania klucza licencyjnego.
2. Wartość umowy w dniu jej zawarcia wynosi:

Cena netto: ……. zł /słownie: ……/100
Cena brutto: ……zł /słownie: ……/100
**Cena ogółem:**
**Cena netto:** ……. zł /słownie: ……/100
**Cena brutto:** ……zł /słownie: ……/100

3. Należność za przedmiot zamówienia płatna będzie w terminie 60 dni od dnia doręczenia faktury do siedziby Zamawiającego. Jako dzień zapłaty przyjmuje się datę obciążenia rachunku bankowego Zamawiającego.
4. Płatność nastąpi na konto Wykonawcy wskazane na fakturze. Wykonawca zobowiązany jest podać na fakturze numer umowy i datę jej zawarcia.
5. Termin zapłaty uważa się za dotrzymany przez Zamawiającego, jeśli rachunek bankowy Zamawiającego zostanie obciążony kwotą należną Wykonawcy najpóźniej w ostatnim dniu terminu płatności.

6. Wykonawca gwarantuje, że jakiekolwiek prawa Wykonawcy związane bezpośrednio lub pośrednio z umową, a w tym wierzytelności Wykonawcy z tytułu wykonania umowy i związane z nimi należności uboczne (m. in. odsetki), nie zostaną przeniesione na rzecz osób trzecich bez poprzedzającej to przeniesienie zgody Zamawiającego wyrażonej w formie pisemnej pod rygorem nieważności. Wykonawca gwarantuje, iż nie dokona jakiejkolwiek czynności prawnej lub też faktycznej, której bezpośrednim lub pośrednim skutkiem będzie zmiana wierzyciela z osoby Wykonawcy na inny podmiot. Niniejsze ograniczenie obejmuje w szczególności przelew, subrogację ustawową oraz umowną, zastaw, hipotekę oraz przekaz. Wykonawca gwarantuje, iż celem dochodzenia jakichkolwiek praw z umowy nie może udzielić upoważnienia, w tym upoważnienia inkasowego, innej firmie, w tym firmie prowadzącej pozostałą finansową działalność usługową, gdzie indziej niesklasyfikowaną, jak i pozostałe doradztwo w zakresie prowadzenia działalności gospodarczej i zarządzania w rozumieniu m.in. przepisów rozporządzenia Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności, tj. firmom zajmującym się działalnością windykacyjną.
7. Wykonawca przyjmuje do wiadomości i zobowiązuje się, iż zapłata za świadczenia wykonane zgodnie z umową nastąpi tylko i wyłącznie przez Zamawiającego bezpośrednio na rzecz Wykonawcy, i tylko w drodze przelewu na rachunek Wykonawcy. Umorzenie długu Zamawiającego do Wykonawcy poprzez uregulowanie w jakiejkolwiek formie na rzecz innych podmiotów niż bezpośrednio na rzecz Wykonawcy, może nastąpić wyłącznie za poprzedzającą to uregulowanie zgodą Zamawiającego wyrażoną w formie pisemnej pod rygorem nieważności.
8. W razie naruszenia obowiązku opisanego wyżej w ustępie 6 Wykonawca zobowiązany będzie do zapłaty na rzecz Zamawiającego kary umownej w wysokości 10 % od ceny ogółem wskazanej jako brutto w § 4 ust. 2 niniejszej umowy za każdy przypadek naruszenia wyżej wskazanego obowiązku, co nie narusza prawa Zamawiającego do dochodzenia odszkodowania przewyższającego wysokość zastrzeżonej kary umownej.
9. W razie naruszenia obowiązku opisanego wyżej w ustępie 7, Wykonawca zobowiązany będzie do zapłaty na rzecz Zamawiającego kary umownej w wysokości 10 % od ceny ogółem wskazanej jako brutto w § 4 ust. 2 niniejszej umowy za każdy przypadek naruszenia wyżej wskazanego obowiązku, co nie narusza prawa Zamawiającego do dochodzenia odszkodowania przewyższającego wysokość zastrzeżonej kary umownej.

**§ 5**

1. Wykonawca przekaże Zamawiającemu klucz licencyjny w terminie zawartym w § 2 ust.4.
2. W przypadku stwierdzenia niezgodności Zamawiający niezwłocznie powiadomi o tym Wykonawcę, który rozpatrzy reklamację w ciągu 2 dni roboczych od dnia jej otrzymania pod nr telefonu …… lub pod nr faksu …… lub na adres e-mail: ……. Zamawiający dodatkowo potwierdzi reklamację pismem poleconym.
3. W przypadku niedotrzymania terminu realizacji przez Wykonawcę Zamawiający dokona wyboru we własnym zakresie innego Wykonawcy i obciąży Wykonawcę z którym została zawarta umowa różnicą w poniesionych kosztach. Uprawnienie to nie wyłącza możliwości domagania się przez Zamawiającego kar umownych określonych w § 7.
4. W przypadku wystąpienia problemów z kompatybilnością zaoferowanego systemu antywirusowego Wykonawca przyjmie na siebie prace związane z procesem dostosowawczym oraz poniesie koszty usunięcia ewentualnych problemów.

**§ 6**

Osobami odpowiedzialnymi na nadzór nad prawidłową realizacją umowy są:

a) ze strony Zamawiającego: Szymon Jurkiewicz – Główny specjalista ds. Informatyki.
b) ze strony Wykonawcy: Pan(i)……

**§ 7**

**Kary umowne**

1. Strony ustalają, że w razie niewykonania lub nienależytego wykonania umowy Wykonawca zapłaci kary umowne:
   a) w wysokości 20% wartości umowy brutto w przypadku odstąpienia od umowy z powodu okoliczności, za które odpowiada Wykonawca;
   b) w wysokości 10% wartości brutto umowy, w przypadku nieterminowego zrealizowania przedmiotu zamówienia;

c) w przypadku niewykonania lub nienależytego wykonania umowy z przyczyn innych niż wymienione w ust. 1 lit. a) do b) Zamawiający naliczy karę umowną w wysokości 10% wartości umowy brutto.

2. Kary wskazane w § 7 ust. 1 naliczane zostaną niezależnie od regulowania zobowiązań finansowych przez Zamawiającego wynikających z umowy.
3. Zamawiający zastrzega sobie prawo dochodzenia odszkodowania uzupełniającego do wysokości rzeczywiście poniesionej szkody.
4. Naliczenie przez Zamawiającego kary umownej następuje poprzez sporządzenie noty księgowej wraz z pisemnym uzasadnieniem. Wykonawca zobowiązany jest w terminie 7 dni od daty otrzymania ww. dokumentów do zapłaty naliczonej kary umownej. Brak zapłaty w powyższym terminie uprawnia Zamawiającego do potrącenia kary umownej z wynagrodzenia Wykonawcy lub innych jego wierzytelności przysługujących Wykonawcy w stosunku do Zamawiającego.
5. Naliczenie przez Zamawiającego bądź zapłata przez Wykonawcę kary umownej nie zwalnia go z zobowiązań wynikających z niniejszej umowy.

**§ 8**
**Postanowienia końcowe**

1. Wykonawca nie może powierzyć wykonania niniejszej umowy innemu podmiotowi.
2. Wszelkie ewentualne sporne sprawy, strony zobowiązują się załatwić polubownie przed sądem właściwym dla siedziby Zamawiającego.
3. W sprawach nieuregulowanych niniejszą umową zastosowanie mają przepisy Kodeksu Cywilnego.
4. Zmiana niniejszej umowy wymaga formy pisemnej pod rygorem nieważności.
5. Zakazuje się istotnych zmian postanowień niniejszej umowy w stosunku do treści oferty, na podstawie, której dokonano wyboru Wykonawcy, za wyjątkiem:
   a) zmiany cen w związku z korzystaniem z rabatów cenowych przyznanych przez Wykonawcę w okresie trwania umowy,
   b) sytuacji, gdy w związku ze zmianą przepisów prawa zmianie ulegnie stawka podatku VAT, Zamawiający dopuszcza zmiany wynagrodzenia o kwotę brutto wynikającą ze zmienionej obowiązującej stawki podatku VAT.
6. Niniejszą umowę wraz z załącznikami sporządzono w 2 jednobrzmiących egzemplarzach, po 1 egzemplarzu dla każdej ze stron.

Załącznik do umowy: Szczegółowy opis przedmiotu zamówienia

**ZAMAWIAJĄCY** **WYKONAWCA**

Załącznik nr 2

# Szczegółowy opis przedmiotu zamówienia

Opis systemu ochrony antywirusowej z zaporą ogniową dla stacji roboczych.

1) Ochrona antywirusowa stacji roboczych:
- Microsoft Windows 7 (32-bit i 64-bit)
- Microsoft Windows 8 (32-bit i 64-bit)
- Microsoft Windows 8.1 (32-bit i 64-bit)
- Microsoft Windows 10

2) Ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli.

3) Komunikacja ochrony antywirusowej z serwerem zarządzania musi odbywać się za pomocą protokołu HTTPS.

4) Możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach.

5) Polski interfejs użytkownika aplikacji ochronnej.

- Opis technologii:

- Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy.
- Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.
- Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan".
- Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie pliku offline ze strony producenta i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.
- Możliwość wywołania skanowania komputera na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
- Możliwość wywołania skanowania komputera w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
- Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.
- Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
- Mikrodefinicje wirusów – przyrostowe (inkrementalne) - pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
- Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.
- Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
- Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
- Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit" oraz ataki typu 0-day
- Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie.
- Ochrona pliku 'hosts' przed niepożądanymi wpisami.
- Mechanizm centralnego zarządzania elementami kwarantanny znajdującymi się na stacjach klienckich.

- Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.
- Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
- Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.
- Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.
- Automatyczne uruchamianie procedur naprawczych.
- Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
- Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).
- Automatyczne powiadomienie użytkowników oraz administratora o wykrytych zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
- Skanowanie przez program na komputerze klienckim przychodzącej i wychodzącej poczty elektronicznej bez konieczności instalowania dodatkowych programów/modułów.
- Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.
- Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
- Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta.
- Automatyczna kwarantanna blokująca ruch przychodzący i wychodzący, włączająca się w momencie, gdy stacja robocza posiada stare sygnatury antywirusowe.
- Wsparcie dla technologii Microsoft Network Access Protection (NAP).
- Ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX i pobieranych plików.
- Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie *Network Interceptor Framework* (niezależnie od rodzaju i wersji przeglądarki).
- Możliwość zabezpieczenia połączenia do witryn skategoryzowanych przez producenta, jako 'bankowość elektroniczna' poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z bankiem.
- Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z daną witryną HTTPS.
- Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez producenta.
- Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji.
- Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.
- Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.
- Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
- Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej)
- Blokowanie dostępu do witryn WWW na podstawie dostarczonych przez producenta kategorii bez konieczności ręcznego wpisywanie poszczególnych adresów.

- Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii musi zostać powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
- Możliwość blokowania witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
- Możliwość blokowania zapytań DNS do witryn sklasyfikowanych, jako niebezpieczne lub podejrzane.
- Możliwość zezwolenia na zapytania DNS tylko do witryn sklasyfikowanych, jako zaufane.
- Brak konieczności restartu komputera po zainstalowaniu aplikacji w środowisku Windows 7/8/8.1
- Moduł kontroli urządzeń zapewniający możliwość zezwolenia lub zablokowania dostępu do urządzeń zewnętrznych (np. napędy USB, urządzenia bluetooth, czytniki kart pamięci, napędy CD/DVD, stacje dyskietek).
- Moduł kontroli urządzeń zarządzany z poziomu konsoli centralnego zarządzania.
- Moduł kontroli urządzeń umożliwia dodanie 'zaufanego urządzenia' poprzez podanie jego identyfikatora sprzętu.
- Moduł aktualizatora aplikacji, który okresowo skanuje i umożliwia aktualizację do najnowszych wersji aplikacji firm trzecich.
- Aktualizator aplikacji spełnia rolę programu łatającego podatności a nie tylko i wyłącznie pasywnego skanera luk w bezpieczeństwie aplikacji.
- Możliwość pobierania instalatorów poprawek bezpośrednio z serwera zarządzającego.
- Administrator ma możliwość wykluczenia aplikacji, które maja nie podlegać aktualizacji poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
- System raportowania powinien pokazywać status podatności aplikacji na komputerach dotyczące całej domeny lub pojedynczych komputerów.
- Aktualizator aplikacji nie może wymagać instalowania dodatkowych agentów oprócz agenta AV.
- Aktualizator powinien dać możliwość aktualizacji poprawek w sposób akcji wymuszonej lub reguły wykonującej się w sposób zaplanowany: dzień, godzina, opcje restartu komputera, wykluczenia aplikacji.
- Administrator konsoli zarządzającej powinien mieć możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
- Aktualizator aplikacji nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces
- Blokowanie aktywności sieciowej związanej ze znanymi botnetami włączając w to ataki ransomware i ataki ukierunkowane

Opis systemu centralnego zarządzania:

1. System centralnego zarządzania może być zainstalowany na wersjach serwerowych Microsoft Windows oraz Linux.
2. Instalacja sytemu centralnego zarządzania dla Microsoft Windows musi wspierać następujące wersje systemów operacyjnych:
   - Windows Server 2008 SP1 32-bit : Standard, Enterprise, Web Server
   - Windows Server 2008 SP1 64-bit: Standard, Enterprise, Web Server, Small Business Server, Essential Business Server
   - Windows Server 2008 R2: Standard, Enterprise, Web Server
   - Windows Server 2012: Essentials, Standard, Datacenter
   - Windows Server 2012 R2: Essentials, Standard, Datacenter
   - Windows 2016 ready
3. Instalacja sytemu centralnego zarządzania dla Linux musi wspierać następujące wersje systemów operacyjnych:
   1. Red Hat Enterprise Linux 5 32/64-bit
   2. Red Hat Enterprise Linux 6 32/64-bit
   3. Red Hat Enterprise Linux 7 32/64-bit
   4. CentOS 6 32/64-bit

5. CentOS 7 32/64-bit
6. SuSE Linux Enterprise Server 10 32/64-bit
7. SuSE Linux Enterprise Server 11 32/64-bit
8. SuSE Linux Enterprise Desktop 11 32/64-bit
9. openSUSE 13.2 32/64-bit
10. Debian GNU Linux 7 (Wheezy) 32/64-bit
11. Debian GNU Linux 8 (Jessie) 32/64-bit
12. Ubuntu 12.04 (Precise Pangolin) 32/64-bit
13. Ubuntu 14.04 (Trusty Tahr) 32/64-bit
14. Ubuntu 16.04 (Xenial Xerus) 32/64-bit

4. Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI) i JAR lub też bezpośrednią instalację zdalną nienadzorowaną.
5. Narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nowe wersję.
6. Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem).
7. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi.
8. Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta.
9. Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.
10. Centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy.
11. Możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów).
12. Tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach.
13. Możliwość importu struktury drzewa z Microsoft Active Directory.
14. Możliwość tworzenia reguł synchronizacji z Microsoft Active Directory umożliwiających automatyczną synchronizację klientów z aktualnie istniejącymi grupami komputerów
15. Możliwość tworzenia reguł powiadamiania o nowych, niezarządzanych klientach w Microsoft Active Directory.
16. Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników.
17. Możliwość zdefiniowania hasła do odinstalowania aplikacji.
18. Możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający.
19. Możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji.
20. Możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta.
21. Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania. Dane muszą być przesyłane do serwera zarządzania podczas kolejnego połączenia.
22. Możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.

23. Umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe.
24. Automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych podczas instalacji.
25. Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej, niż co 7 dni (zalecane codzienne aktualizacje).
26. Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe.
27. Możliwość eksportu raportów z pracy systemu do pliku HTML.
28. Możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich.
29. Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie".
30. Program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa.
31. Program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe.
32. Program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy).
33. Program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów.
34. Dedykowany system raportowania dostępny przez przeglądarkę internetową umożliwiający podgląd statystyk dotyczących wykrytych wirusów, przeprowadzonych ataków, zainstalowanego oprogramowania oraz statystyk połączenia stacji klienckich.
35. System raportowania umożliwiający wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora.
36. Zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania.
37. Możliwość przekierowania alertów bezpośrednio do serwera Syslog.
38. Możliwość tworzenia wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).
39. System umożliwiający wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączania programu.
40. Pełna kopia bazy danych systemu zarządzania centralnego może być wykonywana automatycznie zgodnie z harmonogramem określonym przez administratora.
41. Administrator ma możliwość określenia liczby kopii bazy danych, jaka będzie przetrzymywana.
42. Możliwość wygenerowania danych diagnostycznych z podpiętych komputerów za pomocą konsoli zarządzającej.
43. Możliwość bezpośredniego pobrania z komputera danych diagnostycznych z poziomu konsoli zarządzającej.
44. Możliwość opisywania wprowadzonej konfiguracji za pomocą notatek umieszczonych w interfejsie graficznym konsoli zarządzającej.

Opis oprogramowania antywirusowego dla systemów typu Windows serwer:

3. Ochrona serwerów:
    4. Microsoft Windows Server 2008
    5. Microsoft Windows Server 2008 R2
    6. Microsoft Small Business Server 2008
    7. Microsoft Small Business Server 2011, Standard edition
    8. Microsoft® Small Business Server 2011, Essentials
    9. Microsoft® Windows Server 2012

10. Microsoft® Windows Server 2012 Essentials
11. Microsoft® Windows Server 2012 R2
12. Microsoft® Windows Server 2012 R2 Essentials
13. Microsoft® Windows Server 2016 Technical Preview

14. Ochrona całego systemu monitorowana i zarządzana z pojedynczej konsoli.
15. Zarządzanie aplikacją poprzez interfejs dostępny przez protokół https.
16. Możliwość określenia adresów sieciowych, z których można zarządzać aplikacją.
17. Możliwość określenia portu, na którym dostępny będzie interfejs zarządzający aplikacją.
18. Integracja z systemem anty wirusowym dla serwerów MS Exchange dostarczanym przez producenta poprzez wspólny lokalny interfejs zarządzający.
19. Co najmniej trzy różne silniki antywirusowe, każdy z dedykowanymi bazami sygnatur, funkcjonujące jednocześnie i skanujące wszystkie dane.
20. Zintegrowany silnik „antyrootkitowy".
21. Co najmniej dwa dedykowane silniki „antyspyware".
22. Możliwość blokowania zapytań DNS do witryn sklasyfikowanych, jako niebezpieczne lub podejrzane.
23. Możliwość zezwolenia na zapytania DNS tylko do witryn sklasyfikowanych, jako zaufane.
24. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.
25. Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
26. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta.
27. Ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX
28. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie *Network Interceptor Framework* (niezależnie od rodzaju i wersji przeglądarki).
29. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie plików i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.
30. Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
31. Możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
32. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.
33. Możliwość wywołania szybkiego skanowania pod kątem programów typu rootkit.
34. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym.
35. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
36. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.
37. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
38. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „wirus", „keylogger", „dialer", „trojan", rootkitami" , „spyware", ataki typu 0-day.
39. Program powinien posiadać kwarantannę wirusów, spyware oraz riskware.
40. Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona.

41. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
42. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.
43. Automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa.
44. Automatyczne uruchamianie procedur naprawczych.
45. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
46. Zarządzanie poprzez przeglądarkę WWW oraz centralnie z poziomu jednolitego systemu centralnego zarządzania dla systemów antywirusowych oferowanych przez producenta.
47. Moduł aktualizatora aplikacji, który okresowo skanuje i umożliwia aktualizację do najnowszych wersji aplikacji firm trzecich.
48. Aktualizator aplikacji spełnia rolę programu łatającego podatności a nie tylko i wyłącznie pasywnego skanera luk w bezpieczeństwie aplikacji.
49. Możliwość pobierania instalatorów poprawek bezpośrednio z serwera zarządzającego.
50. Administrator ma możliwość wykluczenia aplikacji, które maja nie podlegać aktualizacji poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
51. Blokowanie aktywności sieciowej związanej ze znanymi botnetami włączając w to ataki ransomware i ataki ukierunkowane.
52. Dezinstalacja oprogramowania antywirusowego na kliencie chroniona hasłem.

Opis oprogramowania antywirusowego z systemem firewall dla systemów Linux:

a. Ochrona stacji roboczych oraz serwerów pracujących pod kontrolą systemu Linux.
b. Ochrona całego systemu monitorowana i zarządzana lokalnie przy pomocy dowolnej przeglądarki WWW.
   Wspierane przeglądarki
   - Mozilla Firefox 38-50
   - Google Chrome 45-53
   - Microsoft Edge
   - Internet Explorer 8, 9, 10, 11
c. Możliwość centralnego zarządzania w sposób zdalny wszystkimi istotnymi funkcjami oprogramowania wraz opcją blokady ustawień.
d. Ochrona systemu realizowana na trzech poziomach, tj.: monitora antywirusowego kontrolującego system w tle, modułu skanującego nośniki danych i osłony internetowej (firewall).
e. Moduł kontrolujący integralność ważnych danych systemowych, automatycznie wykrywający wszelkie próby ich modyfikacji oraz alarmuje administratora
f. Co najmniej trzy różne silniki antywirusowe, każdy z dedykowanymi bazami sygnatur, funkcjonujące jednocześnie i skanujące wszystkie dane.
g. Zapewnia ochronę w czasie rzeczywistym : skanowanie wirusów, sprawdzanie integralności oraz ochronę przed rootkitami
h. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie plików i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.
i. Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.
j. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
k. Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej)
l. Możliwość wywołania skanowania na żądanie, po aktualizacji definicji wirusów lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
m. Możliwość wykluczenia ze skanowania wybranych plików lub folderów

n. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym.
o. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
p. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
q. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „wirus", „keylogger", „dialer", „trojan", „worm".
r. Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona.
s. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.
t. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
u. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.
v. Automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa.
w. Automatyczne uruchamianie procedur naprawczych.
x. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
y. Gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin.
z. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).
aa. Automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy serwer/stacja robocza jest odpowiednio zabezpieczona.
bb. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli lub dedykowanego proxy
cc. Możliwość instalacji na następujących systemach operacyjnych:
32bit:
-CentOS 6.7-6.8
-Debian 7.10-7.11
-Debian 8.5, 8.6 **
-Oracle Linux 6.7, 6.8 RHCK*
-Red Hat Enterprise Linux 6.7-6.8
-SUSE Linux Enterprise Server 11 SP1, SP3, SP4
-Ubuntu 14.04.(4-5),16.04, 16.04.(1-2)
64bit (AMD64/EM64T):
-CentOS 6.7, 6.8, 7.1-1503, 7.2-1511, 7.3
-Amazon Linux 2017.03
-Debian 7.10-7.11
-Debian 8.5, 8.6
-Oracle Linux 6.7, 6.8 RHCK
-Oracle Linux 7.2, 7.3 UEK
-RHEL 6.7-6.8, 7.2-7.3
-SUSE Linux Enterprise Server 11 SP3, SP4
-SUSE Linux Enterprise Server 12, 12 SP4
-Ubuntu 12.04.(1-5), 14.04.(1-3)

Wymagania dotyczące systemu ochrony maszyn wirtualnych:

45. System ochrony maszyn wirtualnych musi wspierać poniższe środowiska wirtualne:
- VMware vSphere 5.1, 5.5, 6.0
- Citrix XenServer 6.2, 6.5
- Microsoft Windows Server 2008 R2, 2012 and 2012 R2 with Hyper-V role
- Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2

46. System ochrony zwirtualizowanych stacji roboczych oraz serwerów musi wspierać poniższe systemy operacyjne:
1. Microsoft Windows Vista
2. Microsoft Windows 7
3. Microsoft Windows 8
4. Microsoft Windows 8.1
5. Microsoft Windows 10
6. Microsoft Windows Server 2008
7. Microsoft Windows Server 2008 R2
8. Microsoft Small Business Server 2008
9. Microsoft Small Business Server 2011, Standard edition
10. Microsoft Small Business Server 2011, Essentials
11. Microsoft Windows Server 2012
12. Microsoft Windows Server 2012 Essentials
13. Microsoft Windows Server 2012 R2
14. Microsoft Windows Server 2016 Technical Preview

47. System umożliwia ochronę zwirtualizowanych stacji roboczych oraz serwerów przed malware, exploitami, atakami sieciowymi oraz innymi zagrożeniami.
48. System umożliwia ochrone w czasie rzeczywistym
49. Rozwiązanie musi umożliwiać poprawę wydajności środowiska wirtualnego poprzez zmniejszenie obciążenia środowiska przez polityki bezpieczeństwa.
50. Rozwiązanie musi umożliwiać przeniesienie obciążenia generowanego przez skanowanie antywirusowe, skanowanie zawartości oraz badanie reputacji na dedykowanego agenta współpracującego z rozwiązaniem.
51. Rozwiązanie musi być dostępne w postaci wirtualnego urządzenia gotowego do instalacji w środowisku wirtualnym.
52. Wielowarstwowa ochrona – zapewnia zaawansowana analizę behawioralną, kontrolę treści internetowej, ochronę przeglądania i zautomatyzowane aktualizacje oprogramowania.

Miejscowość ..... dnia ..... 2019r.

.....

Podpis osoby/osób upoważnionej/upoważnionych

do reprezentowania Wykonawcy