Projekt realizowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego dla Województwa Dolnośląskiego na lata 2014-2020

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

(SPECYFIKACJA TECHNICZNA SPRZĘTU)

ZAŁĄCZNIK NR 2

DO ZAPYTANIA OFERTOWEGO NR 1/2016
z dnia 21 lipca 2017 roku

Projekt „Wdrożenie e-usług w obszarze ochrony zdrowia w placówkach medycznych NZOZ Centrum IKAR we Wrocławiu" dofinansowany w ramach działania 2.1 E-usługi publiczne, poddziałania 2.1.2 E-usługi publiczne – ZIT WROF w ramach Regionalnego Programu Operacyjnego Województwa Dolnośląskiego na lata 2014-2020

1 Informacje ogólne 3

2 Dostawa sprzętu komputerowego 4

2.1 Komputery 4

2.1.1 Komputer wraz z oprogramowaniem oraz sprzętem peryferyjnym 4

2.1.2 Drukarki 5

2.2 Architektura serwerowa 6

2.2.1 Serwer 6

2.2.2 Oprogramowanie do serwerów 7

2.2.2.1 Windows Server Standard 2016 PL x64 16Core x 3 szt 7

2.2.2.2 Microsoft OEM Win CAL 2016 Device PL 5Clt x4 (w sumie 20 licencji dostępowych na końcówki) 8

2.3 Urządzenie do monitorowania sieci (3 szt.) 8

3 Programy antywirusowe dla 15 stanowisk i serwerów 16

1 Informacje ogólne

Przedmiotem zamówienia jest zakup i wdrożenie systemu informatycznego zapewniającego dostęp do wysokiej jakości e-usług w obszarze ochrony zdrowia w placówkach medycznych NZOZ Centrum IKAR we Wrocławiu.

Projekt realizowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego dla Województwa Dolnośląskiego na lata 2014-2020

2 Dostawa sprzętu komputerowego

Sprzęt komputerowy tj. 13 zestawów złożonych z komputera z systemem operacyjnym, zintegrowaną nagrywarką DVD, monitorem 21.5` i drukarką laserową monochromatyczną

2.1 Komputery

2.1.1 Komputer wraz z oprogramowaniem oraz sprzętem peryferyjnym

Przekątna ekranu	21.5"
Proporcje obrazu	16:9
Rozdzielczość	1920 x 1080 (HD 1080)
Ekran dotykowy	Nie
Rodzina procesora	Intel Core i3
Generacja procesora	Szósta
Obsługa ECC	Nie
Taktowanie procesora	2.3 GHz
Pozostałe informacje o procesorze	Intel® Core™ i3-6100U
Zainstalowana pamięć RAM	4 GB
Maks. wielkość pamięci	16 GB
Liczba obsadzonych gniazd pamięci	1
Liczba wolnych gniazd pamięci	1
Rodzaj pamięci	SODIMM DDR4
Częstotliwość szyny pamięci	2133 MHz
Typ dysku	SSHD
Pojemność SSHD	1008 GB
Format szerokości	2,5'' (SFF)
Interfejs dysku	SATA III - 6 Gb/s
Prędkość obrotowa	5400 obr/min
Model karty graficznej	Intel HD Graphics
Porty wideo	1 x HDMI

Interfejs sieciowy	1 x 10/100/1000 Mbit/s Wi-Fi 802.11a/b/g/n/ac Bluetooth
Napęd optyczny	DVD-RW
Liczba portów USB	5
W tym USB 3.0	2
Pozostałe porty we/wy	1 x Audio (Combo) 1 x RJ-45
Kamera internetowa	Tak
Kolor	Czarny
Obudowa	All-In-One
System operacyjny	Windows 10 Pro 64-bit

2.1.2 Drukarki

Rodzaj druku	Laserowy
Format druku	A4
Druk w kolorze	Nie
Rozdzielczość druku	1200 x 600 dpi
Maks. prędkość druku w czerni	28 str/min
Druk Photo	Nie
Druk dwustronny	Automatyczny
Obciążenie miesięczne	20000 arkuszy/miesiąc
Język drukarki	PCL 5e/5c/6
Zainstalowana pamięć	128 MB
Maksymalna pamięć	128 MB
Podajnik papieru	Pojemność wejściowa papieru Maks. (LT/A4): 300
Odbiornik papieru	Pojemność wyjściowa papieru Maks. (LT/A4): 125
Rodzaj nośnika	• Papier • Papier cienki

	• Papier gruby
Gramatura papieru (min.)	52 g/m²
Gramatura papieru (maks.)	162 g/m²
Obsługiwane systemy operacyjne	• Windows XP • Windows Server 2003 • Windows Vista • Windows Server 2008 • Windows 7 • Windows 8
Ethernet	10/100 Mb/s
Komunikacja bezprzewodowa	Nie
Złącza	1 x USB 3.0

2.2 Architektura serwerowa

2.2.1 Serwer

Zestaw układów	Intel® C202
Seria procesora	• Intel Xeon E3 • Intel Xeon E3-1200 v5
Taktowanie procesora	3.1 GHz
Liczba zainstalowanych procesorów	1 szt.
Maks. obsługiwana liczba procesorów	1 szt.
Pozostałe informacje o procesorze	Intel® Xeon® E3-1220 v5 3.0GHz, 8M cache, 4C/8T, turbo (80W)
Typ pamięci	DDR4
Rodzaj pamięci	• Unbuffered • ECC • Single rank
Zainstalowana pamięć RAM	16 GB
Maks. wielkość pamięci	32 GB
Liczba obsadzonych gniazd pamięci	1
Liczba wszystkich gniazd pamięci	4
Interfejs dysku	SATA
Format szerokości	3,5'' (LFF)

Obsługa hot-swap dysków	Nie
Liczba zainstalowanych dysków tw.	2
Maks. liczba dysków w obecnej konfiguracji	4
Pojemność sumaryczna wszystkich zainstalowanych dysków	2 TB
Kontroler dysków	Software
Poziomy RAID	• 0 • 1 • 10 (1+0) • 5
Podtrzymanie bateryjne	Nie
Pozostałe informacje o kontrolerze	S130, programowy RAID (tylko do systemów operacyjnych firmy Microsoft) RAID 0,1,5,10
Typ zintegrowanej karty graficznej	Matrox G200eW z 16 MB pamięci
Napęd optyczny	DVD-RW
Gniazda rozszerzeń	1x PCI-Ex16 Gen3 połówkowej wysokości, połówkowej długości 1x PCI-Ex8 Gen3 połówkowej wysokości, połówkowej długości
Interfejs sieciowy	Jedna dwuportowa gigabitowa karta sieciowa Broadcom BCM 5716
Zewnętrzne porty we-wy	Szeregowy - Sieciowy - Grafika - 2 USB - 5 (2 tył, 2 przód, 1 wew)
Obudowa	Rack 1U
Liczba zamontowanych zasilaczy	1
Maksymalna liczba zasilaczy	1
Moc zasilacza (zasilaczy)	250 W
Obsługa hot-plug zasilaczy	Nie
Informacje o gwarancji	3 lata NBD

2.2.2 Oprogramowanie do serwerów

2.2.2.1 Windows Server Standard 2016 PL x64 16Core x 3 szt

Rodzaj	Serwerowe

Licencja	Na rdzenie
Szczegóły licencji	- Licencja podstawowa, dostarczana na nośniku wraz z kluczem produktu - Licencja na fizyczny rdzeń- minimum 8 rdzeni/procesor - Wymagane dodatkowo licencje dostępowe WS 2016 CAL User/Device. - Jedna licencja obejmuje 16 rdzeni w serwerze, na kolejne fizyczne rdzenie jest wymagana licencja Windows Server Standard 2016 Additional Licence - Prawo do uruchomienia dwóch maszyn wirtualnych z systemem operacyjnym Windows Server lub dwóch Hyper-V kontenerów
Architektura	64-bit
Nośnik	DVD
Wersja językowa	Polska

2.2.2.2 Microsoft OEM Win CAL 2016 Device PL 5Clt x4 (w sumie 20 licencji dostępowych na końcówki)

Rodzaj	Serwerowe
Licencja	CAL
Liczba stanowisk / jednostek	5
Szczegóły licencji	5 Clt Device
Wersja językowa	Polska

2.3 Urządzenie do monitorowania sieci (3 szt.)

OBSŁUGA SIECI

Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.

Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.

Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (część jako router, a część jako bridge).

Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.

Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u.

Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).

Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).

INTRUSION PREVENTION SYSTEM (IPS)

System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.

Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy.

Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.

Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej.

Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.

Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.

Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.

Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).

Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).

Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.

Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.

Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.

OCHRONA ANTYSPAM

Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).

Ochrona antyspam ma działać w oparciu o:

białe/czarne listy,

DNS RBL,

heurystyczny skaner.

W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.

Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWANTE (VPN)

Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).

Odpowiednio kanały VPN można budować w oparciu o:

PPTP VPN,

IPSec VPN,

SSL VPN

SSL VPN musi działać w trybach Tunel i Portal.

Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).

Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.

Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.

FILTR DOSTĘPU DO STRON WWW

Urządzenie ma posiadać wbudowany filtr URL.

Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.

Administrator musi mieć możliwość dodawania własnych kategorii URL.

Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.

Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.

Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:

blokowanie dostępu do adresu URL,

zezwolenie na dostęp do adresu URL,

blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.

Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.

Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.

Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.

Urządzenie posiada możliwość identyfikacji oraz blokowanie przesyłanych danych z wykorzystaniem typu MIME.

Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.

UWIERZYTELNIANIE

Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:

lokalną bazę użytkowników (wewnętrzny LDAP),

zewnętrzną bazę użytkowników (zewnętrzny LDAP),

usługę katalogową Microsoft Active Directory.

Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia

autoryzacje w oparciu o protokoły:

SSL,

Radius,

Kerberos.

Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Active Directory.

Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.

Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI OD DOSTAWCÓW USŁUG INTERNETOWYCH (ISP).

Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).

Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:

równoważenie względem adresu źródłowego,

równoważenie względem adresu źródłowego i docelowego (połączenia).

Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do internetu.

Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

Urządzenie ma posiadać mechanizm statycznego trasowania pakietów.

Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.

POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA

Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.

Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.

Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.

Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS

Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.

Urządzenie musi posiadać usługę DNS Proxy.

ADMINISTRACJA URZĄDZENIEM

Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.

Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.

Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.

Komunikacja może odbywać się na porcie innym niż https (443 TCP).

Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.

Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog).

Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.

Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.

RAPORTOWANIE

Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.

System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.

System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów.

System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu.

W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.

Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy

PARAMETRY SPRZĘTOWE

Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać z wbudowanej pamięci flash.

Liczba portów Ethernet 10/100/1000 – min. 5 w tym min. 2 routowalne

Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G.

Przepustowość Firewalla – min. 400 Mbps

Przepustowość Firewalla wraz z włączonym systemem IPS – min. 200 Mbps.

Przepustowość filtrowania Antywirusowego – min. 55 Mbps

Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 100 Mbps.

Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 25.

Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 5.

Obsługa min. 50 VLAN-ów.

Liczba równoczesnych sesji - min. 30 000 i nie mniej niż 2 500 nowych sesji/sekundę.

Urządzenie jest nielimitowane na użytkowników.

Serwis 5 lat

3 Programy antywirusowe dla 15 stanowisk i serwerów

Skrócona specyfikacja ESET Endpoint antivirus suite

1. Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10
2. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.
3. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives.

Ochrona antywirusowa i antyspyware

4. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
5. Wbudowana technologia do ochrony przed rootkitami.
6. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
9. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami
10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
11. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
12. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
13. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
14. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
15. 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.
16. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
17. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
18. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
19. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
20. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
21. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony

internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.

22. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
23. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
24. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
25. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
26. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
27. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
28. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
29. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
30. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
31. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
32. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
33. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
34. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
35. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
36. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
37. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu.
38. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
39. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.

40. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
41. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
42. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
43. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
44. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
45. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
46. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
47. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
48. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
49. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
50. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
51. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
52. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
53. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
54. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
55. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
56. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.
57. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
58. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
59. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.

Ochrona serwera plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016, SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012.
2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
4. Wbudowana technologia do ochrony przed rootkitami i exploitami.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
8. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
9. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.
13. Aplikacja powinna wspierać mechanizm klastrowania.
14. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
15. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
16. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
17. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia.
18. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.
19. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
20. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
21. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
22. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
23. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
24. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
25. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
26. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
27. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).

28. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
29. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
30. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
31. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
32. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail.
33. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
34. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.
35. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.
36. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
37. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
38. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
39. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
40. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
41. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
42. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
43. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
44. Aplikacja musi wspierać skanowanie magazynu Hyper-V
45. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów

46. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).
47. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
48. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

Administracja zdalna

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012 oraz systemach Linux.
2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).
3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.
4. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.
5. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
6. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
7. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.
8. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
9. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
10. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
11. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.
12. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
13. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
14. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
15. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
16. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
17. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
18. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.

19. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
20. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
21. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
22. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
23. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
24. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.
25. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
26. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
27. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
28. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
29. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
30. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
31. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
32. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
33. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
34. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
35. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
36. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
37. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.
38. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.
39. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.

40. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.
41. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
42. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
43. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.
44. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
45. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
46. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
47. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
48. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
49. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
50. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
51. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
52. Serwer administracyjny musi być wyposażona w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.
53. Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie).