## Załącznik nr 1

FORMULARZ OFERTY WYKONAWCY

|  |  |
| --- | --- |
| **Parametr lub warunek** | **Minimalne wymagania** |
| **Serwer** |
| Obudowa | -Typu Rack, wysokość maksimum 2U;-Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack oraz ramieniem porządkującym przewody za serwerem; |
| Płyta główna | -Wieloprocesorowa (2 lub 4 procesorowa), wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów 28-rdzeniowych;-Wyposażona w minimum 24 gniazda pamięci RAM DDR4, obsługa minimum 3000GB pamięci RAM DDR4 2933 Mhz;-Oferowany model serwera musi obsługiwać pamięć nieulotną instalowaną w gniazdach pamięci RAM o pojemności sumarycznej minimum 1000GB (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci) – minimum 12 gniazd pamięci RAM musi umożliwiać wymienną instalację tego typu modułów;-Sumarycznie minimum 6 złącz PCI Express generacji 3, w tym minimum 3 złącza o prędkości x16;-Aktywne min. 3 sloty PCI Express, w tym minimum 1 złącze o prędkości x16;-Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; -Zintegrowany moduł TPM 2.0; |
| Procesory | -Zainstalowany jeden procesor 8-rdzeniowy w architekturze x86, taktowany podstawowym zegarem min. 2,1 GHz, osiągający wynik (w konfiguracji dwuprocesorowej) w testach wydajności SPECrate2017\_int\_base min. 81,4 pkt. Wynik dla oferowanego modelu serwera wraz z oferowanym modelem procesora dostępny na stronie spec.org; |
| Pamięć RAM | -Zainstalowane 64 GB pamięci RAM typu DDR4 Registered, 2933Mhz w kościach o pojemności 32 GB;-Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC;-Wsparcie dla konfiguracji pamięci w trybie „Rank Sparing” |
| Kontrolery dyskowe, I/O | -Zainstalowany kontroler SAS 3.0 obsługujący poziomy RAID 0,1,5,10,50; |
| Dyski twarde | -Zainstalowane min. 2 dyski SSD SATA 6G o pojemności 480GBGB każdy,-Zainstalowane min. 2 dyski SATA 6Gb/s o pojemności 2 TB każdy, o prędkości 7,2k RPM dyski Hotplug;-Minimum 8 wnęk dla dysków twardych Hotplug 2,5”. Możliwość rozbudowy do 16 zatok na dyski 2,5”. |
| Inne napędy zintegrowane | -Możliwość instalacji wewnętrznego napędu LTO-6 SAS lub LTO-7 SAS. Alternatywnie dopuszcza się zaoferowanie dodatkowej obudowy rack max 1U dla napędu LTO6/7 wyposażonej w nadmiarowe zasilacze hotplug i okablowanie oraz dostarczenie oferowanego serwera wraz z zainstalowanym kontrolerem SAS HBA umożliwiającym podłączenie i poprawną pracę oferowanej obudowy wyposażonej w napęd LTO-6 lub LTO-7 z oferowanym serwerem; Obudowa musi być objęta jednolitym serwisem takim jak oferowany serwer;-Zainstalowany fabrycznie wewnętrzny napęd DVD-RW; |
| Kontrolery LAN | -Jedna dwuportowa karta 2 x 1 Gbit/s ze wsparciem iSCSI, niezajmująca slotu PCI Express;-Możliwość instalacji osobnej karty sieciowej wyposażonej w porty 2 x 10 Gbit/s SFP+ lub 2 x 10 Gbit/s RJ-45 lub 4 x 10 Gbit/s SFP+ lub 4 x 1 Gbit/s RJ-45, karta niezajmująca slotu PCI Express (dopuszcza się instalację w slocie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilością slotów PCI Express); |
| Kontrolery I/O FC/SAS/Inne | -Brak |
| Porty | -zintegrowana karta graficzna ze złączem VGA wyprowadzonym na tył oraz przód obudowy sewera;-2x USB 3.0 dostępne na froncie obudowy-2x USB 3.0 dostępne z tyłu serwera-1x USB 3.0 wewnątrz serweraIlość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera; |
| Zasilanie, chłodzenie | -Redundantne zasilacze hotplug o mocy minimum 800W każdy, o sprawności 94%;-Redundantne wentylatory hotplug; -Dostarczone wraz z kablami C13-C14 o długości min. 4m każdy; |
| Zarządzanie | -Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system przewidywania/rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zrządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera;Wymaga się aby system przewidywania/rozpoznawania awarii był niezależny i działał w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym.-Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:* Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
* Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
* Dostęp poprzez przeglądarkę Web (także SSL, SSH)
* Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii
* Zarządzanie alarmami (zdarzenia poprzez SNMP)
* Możliwość przejęcia konsoli tekstowej
* Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)
* Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych)
* Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 16Gbit/s oferowanych przez producenta serwera)
* Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
* Dedykowana, wbudowana w kartę zarządzającą pamięć flash o pojemności minimum 16 GB
* Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB);
* Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania;
* Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
* Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji;
* Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń);
* Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą;
* Karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera;
 |
| Wspierane OS | -Windows Server 2019, Windows Server 2016, Windows 2019 Hyper-V, Windows 2016 Hyper-V, VMware, Suse, RHEL |
|  |  |
| Gwarancja | -5 lat gwarancji producenta serwera w trybie onsite z czasem reakcji najpóźniej w następnym dniu roboczym od zgłoszenia usterki;-Dostępność części zamiennych przez 5 lat od momentu zakupu serwera;-Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji; |
| Dokumentacja, inne | - Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone do oferty).- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Unii Europejskiej - Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg;- Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu w języku polskim lub angielskim;- Ogólnopolska, telefoniczna linia techniczna producenta serwera (ogólnopolski numer stacjonarny lub o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) umożliwiająca w czasie obowiązywania gwarancji na sprzęt po podaniu numeru seryjnego urządzenia: zgłoszenie usterki sprzętowej urządzenia oraz weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji – obsługa w języku polskim, w trybie całodobowym również w dni świąteczne;-Wymagane jest oświadczenie Producenta oferowanego serwera, iż wymagany w postepowaniu poziom gwarancji i wsparcia na sprzęt i oferowane wraz z nim oprogramowanie został zaaferowany przez Producenta serwera na potrzeby oferty w niniejszym postępowaniu;-Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;-Wszystkie parametry i funkcje oferowanego serwera muszą być wspierane przez producenta i zaimplementowane fabrycznie oraz dostępne w seryjnej produkcji danego modelu urządzenia. Zamawiający nie dopuszcza dostosowywania funkcji na potrzeby niniejszego postępowania.-Wszystkie parametry i funkcje oferowanego serwera muszą być potwierdzone w ogólnodostępnej dokumentacji producenta. |

**Wycena:**

**Cena jednostkowa: …………………………………**

**wartość brutto: ……………………………………..**

|  |
| --- |
| **System operacyjny 1 szt** |
| **Minimalne wymagania** |
| Wymagane dostarczenie licencji na oprogramowanie Windows Server 2019 Standard, dla serwera będącego podmiotem postępowania, jako oryginalne nieotwierane wcześniej, zafoliowane fabrycznie, bądź zaklejone fabrycznie, opakowania kartonowe, z nośnikiem optycznym lub bez, z hologramem lub zabezpieczeniem innego rodzaju i załączoną w środku kartą lub naklejką z nadrukowanym, nieupublicznionym, nieużywanym, nieaktywowanym i niesprzedawanym nigdy wcześniej kluczem aktywacyjnym, |

**Wycena:**

**Cena jednostkowa: …………………………………**

**wartość brutto: ……………………………………..**

|  |
| --- |
| **Licencja dostępu do serwera, dla użytkownika - 30 szt.** |
| **Minimalne wymagania:** |
| Licencja dla użytkownika, który korzysta z usług serwera, bez względu na liczbę urządzeń, za pomocą których użytkownik korzysta z tych usług, zgodna z systemem operacyjnym Windows Server 2016 oraz Windows Server 2019; |

**Wycena:**

**Cena jednostkowa: …………………………………**

**wartość brutto: ……………………………………..**

|  |
| --- |
| **Licencje serwera pulpitu zdalnego – RDS CAL – 5 szt.** |
| **Minimalne wymagania:** |
| Licencja przypisywana do użytkownika lub urządzenia umożliwiająca dostęp do serwera poprzez zdalne połączenie za pomocą protokołu RDP. Licencja zgodna z systemem operacyjnym Windows Server 2019; |

**Wycena:**

**Cena jednostkowa: …………………………………**

**wartość brutto: ……………………………………..**

|  |
| --- |
| **Licencje systemu antywirusowego wersja serweraowa 2 szt.** |
| **Minimalne wymagania:** |
| 1. Ochrona serwerów:
	1. Microsoft Windows Server 2008 R2
	2. Microsoft Small Business Server 2008
	3. Microsoft Small Business Server 2011, Standard edition
	4. Microsoft® Small Business Server 2011, Essentials
	5. Microsoft® Windows Server 2012
	6. Microsoft® Windows Server 2012 Essentials
	7. Microsoft® Windows Server 2012 R2
	8. Microsoft® Windows Server 2012 R2 Essentials
	9. Microsoft® Windows Server 2016 Technical Preview
2. Ochrona całego systemu monitorowana i zarządzana z pojedynczej konsoli.
3. Zarządzanie aplikacją poprzez interfejs dostępny przez protokół https.
4. Możliwość określenia adresów sieciowych, z których można zarządzać aplikacją.
5. Możliwość określenia portu, na którym dostępny będzie interfejs zarządzający aplikacją.
6. Integracja z systemem anty wirusowym dla serwerów MS Exchange dostarczanym przez producenta poprzez wspólny lokalny interfejs zarządzający.
7. Co najmniej trzy różne silniki antywirusowe, każdy z dedykowanymi bazami sygnatur, funkcjonujące jednocześnie i skanujące wszystkie dane.
8. Zintegrowany silnik „antyrootkitowy”.
9. Co najmniej dwa dedykowane silniki „antyspyware”.
10. Możliwość blokowania zapytań DNS do witryn sklasyfikowanych, jako niebezpieczne lub podejrzane.
11. Możliwość zezwolenia na zapytania DNS tylko do witryn sklasyfikowanych, jako zaufane.
12. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.
13. Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
14. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta.
15. Ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX
16. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie *Network Interceptor Framework* (niezależnie od rodzaju i wersji przeglądarki).
17. 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.
18. Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
19. Możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
20. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.
21. Możliwość wywołania szybkiego skanowania pod kątem programów typu rootkit.
22. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym.
23. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
24. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.
25. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
26. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „wirus”, „keylogger”, „dialer”, „trojan”, rootkitami” , „spyware”, ataki typu 0-day.
27. Program powinien posiadać kwarantannę wirusów, spyware oraz riskware.
28. 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.
29. 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).
30. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.
31. Automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa.
32. Automatyczne uruchamianie procedur naprawczych.
33. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
34. Zarządzanie poprzez przeglądarkę WWW oraz centralnie z poziomu jednolitego systemu centralnego zarządzania dla systemów antywirusowych oferowanych przez producenta.
35. Moduł aktualizatora aplikacji, który okresowo skanuje i umożliwia aktualizację do najnowszych wersji aplikacji firm trzecich.
36. Aktualizator aplikacji spełnia rolę programu łatającego podatności a nie tylko i wyłącznie pasywnego skanera luk w bezpieczeństwie aplikacji.
37. Możliwość pobierania instalatorów poprawek bezpośrednio z serwera zarządzającego.
38. Administrator ma możliwość wykluczenia aplikacji, które maja nie podlegać aktualizacji poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
39. Blokowanie aktywności sieciowej związanej ze znanymi botnetami włączając w to ataki ransomware i ataki ukierunkowane.
40. Dezinstalacja oprogramowania antywirusowego na kliencie chroniona hasłem.
 |

**Wycena:**

**Cena jednostkowa: …………………………………**

**wartość brutto: ……………………………………..**

|  |
| --- |
| **Licencje systemu antywirusowego stacje klienckie 30 szt.** |
| **Minimalne wymagania:** |
| **Istotne cechy oprogramowania:**1. Ochrona antywirusowa stacji roboczych:

- Microsoft Windows 7 (32-bit i 64-bit)- Microsoft Windows 7 with SP1 or newer (32-bit i 64-bit)- Microsoft Windows 8 oraz 8.1 (32-bit i 64-bit)- Microsoft Windows 10- MacOS version 10.14 "Mojave"- Mac OS X version 10.13 (El Capitan)- Mac OS X version 10.12 (Sierra)1. Ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.
2. Wspierane przeglądarki internetowe:

- Microsoft Internet Explorer- Microsoft Edge- Mozilla Firefox- Google Chrome- Safari1. Polski interfejs użytkownika

**Wymagania dotyczące technologii:**1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy.
2. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.
3. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”.
4. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
5. Możliwość dystrybuowania aktualizacji za pomocą serwera pośredniczącego. Serwer pośredniczący pobiera aktualizacje oprogramowania, jak i bazy antywirusowe, z serwerów producenta, a następnie dystrybuuje je w sieci lokalnej.
6. Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
7. Możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
8. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.
9. Możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
10. Możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
11. Możliwość skanowania dysków przenośnych takich jak dyski USB, dyski zewnętrzne, drukarki czy dyski sieciowe.
12. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
13. Skanowanie na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
14. 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).
15. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
16. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
17. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”, „rootkit”.
18. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger”, „dialer”, „trojan” w kwarantannie.
19. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.
20. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.
21. Ochrona pliku HOSTS, przed nieautoryzowaną zmianą.
22. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.
23. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.
24. Automatyczne uruchamianie procedur naprawczych.
25. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
26. Automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem stacja robocza jest odpowiednio zabezpieczona.
27. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.
28. Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
29. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
30. Ochrona przeglądarki internetowej, w tym: analiza uruchamianych skryptów ActiveX i pobieranych plików.
31. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie *Network Interceptor Framework* (niezależnie od rodzaju i wersji przeglądarki).
32. Możliwość zabezpieczenia połączenia do witryn skategoryzowanych przez producenta, jako ‘bankowość elektroniczna’ poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z bankiem.
33. 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.
34. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.
35. Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.
36. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
37. Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej)
38. Blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy reputacyjne producenta. Brak konieczności ręcznego wpisywania poszczególnych adresów.
39. 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.
40. Możliwość blokowania witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
41. Brak konieczności restartu systemu operacyjnego po zainstalowaniu aplikacji w środowisku Windows 7/8/8.1/10
42. Dostępne narzędzie do zdalnej instalacji produktu w sieci lokalnej.
43. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana.
44. Możliwość blokowania ustawień konfiguracyjnych stacji roboczych z poziomu portalu zarządzającego w celu uniemożliwienia ich modyfikacji przez użytkowników.
45. Portal zarządzający musi pozwalać na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (telefony komórkowe, smartphony).
46. Portal zarządzający dostępny w języku polskim.
47. Możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
48. Możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
49. Możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.
50. Moduł aktualizatora aplikacji, który okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
51. Aktualizator aplikacji musi spełniać role programu łatającego podatności i instalującego aktualizacje oprogramowania, a nie tylko i wyłącznie pasywnego skanera luk w bezpieczeństwie aplikacji.
52. Administrator ma możliwość wykluczenia aplikacji, które maja nie podlegać aktualizacji poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
53. System centralnego zarządzania musi prezentować niezaktualizowane aplikacje na komputerach dotyczące całej domeny lub listę nieaktualizowane oprogramowania na pojedynczej stacji końcowej.
54. Aktualizator aplikacji nie może wymagać instalowania dodatkowych agentów oprócz agenta AV.
55. Aktualizator powinien dać możliwość wymuszenia instalacji aktualizacji w sposób akcji wymuszonej z poziomu interfejsu zarządzania lub reguły wykonującej się w sposób zaplanowany: dzień, godzina, opcje restartu komputera, wykluczenia aplikacji.
56. 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.
57. Aktualizator aplikacji nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
58. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
59. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.
60. Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.
61. Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
62. Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
63. Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
64. Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.
 |

**Wycena:**

**Cena jednostkowa: …………………………………**

**wartość brutto: ……………………………………..**

|  |
| --- |
| **Serwer sieciowy NAS 1 szt.** |
| **Minimalne wymagania:** |
| **Kieszenie na dyski** 2,5"/3,5" - 2 szt. (Hot swap)**RAID** 01JBODSingle Disk**Rodzaje wyjść / wejść**USB 3.0 - 2 szt.USB 2.0 - 2 szt.RJ-45 10/100/1000 (LAN) - 2 szt.DC-in (wejście zasilania) - 1 szt.**Procesor**Intel Celeron (4 rdzenie, 2.0 GHz do 2.42 GHz)**Pamięć RAM**2 GB (DDR3)**Protokoły sieciowe**AFP, Dynamiczny DNS (DDNS), http, HTTPS, iSCSI, Klient DHCP lub statyczny adres IP,Klient NTP, Klient protokołu BitTorrent, NTP, Obsługa ramek typu jumbo, Serwer CIFS/SMB,Serwer DHCP,Serwer, FTP, Serwer iTunes,Serwer NFS,Serwer WWW,SNMP, SSH, Telnet**System plików dla dysków zewnętrznych**FAT32,NTFS, HFS+,EXT3,EXT4**Dodatkowe informacje**Dostęp przez sieć WebObsługa serwera iTunesObsługa serwera FTPObsługa serwerów multimedialnych UPnP (obsługa platform PS3, Xbox)Surveillance Station - obsługa kamer IPSzyfrowanie woluminówZabezpieczenie Kensington lock |

**Wycena:**

**Cena jednostkowa: …………………………………**

**wartość brutto: ……………………………………..**

|  |
| --- |
| **Dyski do serwera NAS 2 szt.** |
| **Minimalne wymagania:** |
| **Pojemność**6000 GB**Format**3.5"**Interfejs**SATA III (6.0 Gb/s) - 1 szt.**Pamięć podręczna cache**256 MB**Prędkość obrotowa**7200 obr./min**Niezawodność MTBF**1 000 000 godz.**Minimalna głośność pracy**29 dB**Wysokość**26 mm**Szerokość**101,6 mm**Głębokość**147 mm**Waga**720 g |

**Wycena:**

**Cena jednostkowa: …………………………………**

**wartość brutto: ……………………………………..**

|  |
| --- |
| **Przełącznik sieciowy 1 szt.** |
| **Minimalne wymagania:** |
| **Typ obudowy**Do szaf RACK**Zarządzanie**Zarządzalny L2**Dostęp**Wiersz poleceń (CLI)SNMP v1/v2c/v3RMONSNTPTelnet**Architektura sieci**Gigabit Ethernet**Całkowita liczba portów**52**Złącza**RJ-45 10/100/1000 Mbps - 48 szt.SFP+ - 4 szt.**Obsługiwane standardy**IEEE 802.3IEEE 802.3 uIEEE 802.3 xIEEE 802.3 abIEEE 802.3 ae**Rozmiar tablicy MAC**16 k**Ramka Jumbo**9,216 B**Liczba grup VLAN**4096**Algorytm przełączania**Store-and-forward**Szybkość przekierowań pakietów**131 Mb/s**Przepustowość**176 Gb/s**Bufor pamięci**3 MB**Warstwa przełączania**2**Materiał obudowy**Metal**Maksymalny pobór mocy**44,2 W**Dodatkowe informacje**Automatyczne krosowanie portów (Auto MDI-MDIX)Automatyczna negocjacja szybkości połączeńAutomatyczne rozpoznawanie kabla krosowego (MDI/MDIX)Praca w trybie half i full-duplexSNMP**Wysokość**44 mm**Szerokość**440 mm**Głębokość**250 mm**Waga**2,4 kg**Dołączone akcesoria**Kabel zasilający |

**Wycena:**

**Cena jednostkowa: …………………………………**

**wartość brutto: ……………………………………..**

|  |
| --- |
| **Szafa sieciowa rack 1 szt.** |
| **Minimalne wymagania:** |
| * **Rodzaj szafy** wolnostojąca
* **Standard RACK** 19-calowy
* **Wysokość robocza [U]** 42U (Unit) / ok. 205cm
* **Wysokość zewnętrzna [mm]** 2055mm
* **Szerokość zewnętrzna [mm]** 800mm
* **Głębokość zewnętrzna [mm]** 800mm
* **Kolor szafy** czarny RAL9004
* **Rodzaj frontów** szkło hartowane
* **Rodzaj drzwi tylnych** pojedyncze - pełna stal
* **Wentylacja** sufitowy panel wentylacyjny (4 wiatraki)
* **Kółka transportowe** 4 kółka + 4 nóżki
* **Organizer pionowy** 2 organizery pionowe
* **Zamek** 4 zamki (drzwi frontowe, drzwi tylne + panele boczne)
 |

**Wycena:**

**Cena jednostkowa: …………………………………**

**wartość brutto: ……………………………………..**

|  |
| --- |
| **Zasilacz awaryjny + dodatkowy batery pack 1 szt.** |
| **Minimalne wymagania:** |
| **Zasilacz awaryjny:**Moc pozorna / Moc czynna : 3000VA (2400W)Rodzaj UPS: Online 1-Fazowy 1/1Power Factor wyjściowy: 0.8Rodzaj Obudowy: Rack 19" / TowerKształt Fali: Pure Sine Wave (Czysta fala sinusoidalna)Wejście / Wyjście: 1x C20 / 4x IEC C13, Terminal (zaciski śrubowe)Ilość oraz rodzaj baterii na wyposażeniu: 6x 12V / 9AhPorty komunikacyjne: RS-232 oraz USBPort EPO: NIEZłącze dodatkowej baterii: TAKZabezpieczenie RJ45: NIEŁadowarka: 1AWydajność: Tryb Line: 90% / Tryb Bateryjny: 88%Zabezpieczenia: przeciwprzepięciowe, przeciwzwarciowe, przeciwprzeciążeniowe,**Batery pack:**Ilość baterii: 12x 12V / 9AhNapięcie na wyjściu: 72VDCWymiary (wys x szer x głęb): 86,5 x 438 x 608 (mm)Waga: 44,5kg. |

**Wycena:**

**Cena jednostkowa: …………………………………**

**wartość brutto: ……………………………………..**

|  |
| --- |
| **System klimatyzacji 1 szt.** |
| **Minimalne wymagania:** |
| **Specyfikacja jednostki wewnętrznej**Wydajność (Chłodzenie) 3,6 (1,0-4,0) [kW]Wydajność (Grzanie) 3,7 (1,1-4,6) [kW]Zdolność usuwania wilgoci 1,6 [l/h]Przepływ powietrza (chłodzenie/grzanie) 550 [m3/h]Poziom ciśnienia akustycznego (Chłodzenie (Q/L/M/H)) 21/29/33/38 [dB(A)]**Dane energetyczne**Klasa efektywności energetycznej (chłodzenie/grzanie) A++/A+Roczne zużycie energii (Chłodzenie/Grzanie) 197/1092 [kWh/rok]SEER\* 6,1EER\* 3,23Pobór mocy (Chłodzenie) 1,11 (0,30-1,50) [kW]Pobór mocy (Grzanie) 0,99 (0,40-1,50) [kW]Temperatura pracy chłodzenie (wew. / zew.) 21-35 / -10-43 [°C]Temperatura pracy grzanie (wew. / zew. 10-27 / -15-24 [°C]Zasilanie 1/230/50 [f/V/Hz]**Specyfikacja jednostki zewnętrznej**Poziom mocy akustycznej dB(A) 63Poziom ciśnienia akustycznego dB(A) 48Prąd roboczy max (A) 6,7Czynnik chłodniczy R32Napełnienie czynnikiem R32 (g) 620Średnica przewodu cieczowego (mm) 6,35Średnica przewodu gazowego (mm) 9,52 |

**Wycena:**

**Cena jednostkowa: …………………………………**

**wartość brutto: ……………………………………..**