Załącznik Nr 3 do SWZ
w postępowaniu
znak: DTG/129/ZP-10/23

Opis przedmiotu zamówienia
w postępowaniu na „dostawę oprogramowania”

Część III – Oprogramowanie 3 (po zmianie)

Legenda:

1. Oferowany przedmiot zamówienia musi być zgodny z opisem.
2. Parametry minimalne są warunkami granicznymi tzn. niespełnienie któregokolwiek z wymienionych parametrów, będzie skutkowało odrzuceniem oferty.
3. Jeżeli w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, lub pochodzenie, a przy tym znaku towarowym znajduje się dopisek *„lub równoważne”,* Zamawiający może zaoferować rozwiązania równoważne do podanych przez Zamawiającego.
4. Kryteria stosowane w celu oceny równoważności: Wykonawca który oferuje rozwiązania równoważne ma obowiązek wykorzystać wszelkie dostępne mu środki w celu wykazania, iż oferowane przez niego rozwiązanie jest równoważne. Wówczas obowiązkiem wykonawcy jest podanie opisu rozwiązania równoważnego. Opis ten musi być na tyle szczegółowy, żeby zamawiający przy ocenie ofert mógł ocenić czy zaproponowane rozwiązania równoważne spełniają jego wymagania i będą należycie spełniały cel postępowania. Opis rozwiązania równoważnego należy podać w niniejszym załączniku i powinien być tak szczegółowy, żeby zamawiający w toku badania ofert mógł stwierdzić, czy zaproponowane rozwiązanie spełnia wymagania zamawiającego.

Wymagane parametry techniczno-użytkowe (minimalne):

Wszystkie licencje muszą być rejestrowane na dane zamawiającego
(Państwowa Akademia Nauk Stosowanych w Krośnie
Rynek 1, 38-400 Krosno
tel. 13-43-755-00
e-mail: aktywacja@pans.krosno.pl
NIP: 6842175051)

L.p.	Oprogramowanie o następujących funkcjach lub równoważne:				
1. Oprogramowanie – 20 szt.		VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa):		23 %			
Subskrypcja na 12 miesięcy. Subskrypcja na urządzenia współużytkowania (pracownie komputerowe) umożliwiająca instalację oprogramowania na komputerach z system operacyjnym Windows i MacOs. Oprogramowanie wchodzące w skład pakietu: - edytor grafiki rastrowej - program do tworzenia i edycji grafiki wektorowej - program do projektowania publikacji drukowanych i cyfrowych - narzędzie do projektowania interfejsów użytkownika (UI) i prototypowania - profesjonalny program do edycji wideo - program do tworzenia efektów specjalnych i animacji - edytor dźwięku i program do miksowania audio - narzędzie do zarządzania i edycji fotografii - program do przeglądania i organizowania plików multimedialnych - program do projektowania i edycji stron internetowych - narzędzie do tworzenia animacji interaktywnych - program do tworzenia, edycji i podpisywania plików PDF - narzędzie do tworzenia grafiki 3D i renderowania - program do animowania postaci na podstawie nagrania wideo - zestaw narzędzi do tworzenia grafiki, filmów i stron internetowych Wymagana instalacja i konfiguracja oprogramowania na sprzęcie wskazanym przez Zamawiającego.					
2. Oprogramowanie – 30 szt.		VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa):		23 %			
Subskrypcja na 12 miesięcy. Subskrypcja oprogramowania posiadanego przez Zamawiającego pod nazwą "Altium Designer" (najnowsza aktualna wersja oferowana przez producenta oprogramowania z dnia składania oferty). Początek obowiązywania subskrypcji październik 2023r. Wymagana instalacja i konfiguracja oprogramowania na sprzęcie wskazanym przez Zamawiającego.					
3. Oprogramowanie – 1 pakiet.		VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa):		23 %			
Subskrypcja na 12 miesięcy. Subskrypcja oprogramowania posiadanego przez Zamawiającego pod nazwą "ArcGIS poziom 2 - dla 50 użytkowników" (najnowsza aktualna wersja oferowana przez producenta oprogramowania z dnia składania oferty). Początek obowiązywania subskrypcji październik 2023 r. Wymagana instalacja i konfiguracja oprogramowania na sprzęcie wskazanym przez Zamawiającego.					
4. Oprogramowanie – 1 pakiet.		VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa): ..... Opis rozwiązania równoważnego (jeśli Wykonawca oferuje rozwiązanie równoważne): ……		23 %			

…… ……				

Subskrypcja na 12 miesięcy. Oprogramowanie pod nazwą "Azure DevTools" lub równoważne (najnowsza aktualna wersja oferowana przez producenta oprogramowania z dnia składania oferty). Początek obowiązywania subskrypcji październik 2023 r. Wymagana instalacja i konfiguracja oprogramowania na sprzęcie wskazanym przez Zamawiającego.

5. Oprogramowanie – 20 szt.	VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa):	23 %			

Oprogramowanie graficzne, wyposażone w zaawansowane narzędzia do tworzenia ilustracji, układu stron, edycji zdjęć. Oprogramowanie umożliwiające projektowanie logotypów, broszur, materiałów sprzedażowych, marketingowych, szkoleniowych, plakatów i innych rodzajów prac. Pakiet oprogramowania: - do projektowania grafiki wektorowej - do edycji zdjęć – do przekształcania map bitowych w edytowalne grafiki wektorowe - do przechwytywania obrazów z ekranu komputera Aplikacje pomocnicze: – pozwalające na szybkie edytowanie zdjęć w formacie RAW (wersja angielska) – umożliwiające animowanie zdjęć (wersja angielska) Wersja językowa: polska Obszar zastosowań: edukacyjna, prowadzenie zajęć z zakresu grafii komputerowej Okres licencji: bezterminowa Platforma: na komputery stacjonarne PC. Najnowsza aktualna wersja oferowana przez producenta oprogramowania z dnia składania oferty. Wymagana instalacja i konfiguracja oprogramowania na sprzęcie wskazanym przez Zamawiającego.

6. Oprogramowanie – 2 szt.	VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa):	23 %			

Subskrypcja na 12 miesięcy. Aktualizacja oprogramowania posiadanego przez zamawiającego pod nazwą "Adobe Creative Cloud All Apps for Teams MULTI Win/Mac." (najnowsza aktualna wersja oferowana przez producenta oprogramowania z dnia składania oferty). Początek obowiązywania subskrypcji październik 2023 r.

7. Oprogramowanie – 4 szt.	VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa):	23 %			

Subskrypcja na 12 miesięcy. Subskrypcja oprogramowania posiadanego przez Zamawiającego pod nazwą "MobaXterm" (najnowsza aktualna wersja oferowana przez producenta oprogramowania z dnia składania oferty). Początek obowiązywania subskrypcji październik 2023 r. Wymagana instalacja i konfiguracja oprogramowania na sprzęcie wskazanym przez Zamawiającego.

8. Oprogramowanie – 1 szt.	VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa):	23 %			

Subskrypcja na 12 miesięcy.
Platforma: na komputery stacjonarne PC.
Subskrypcja na użytkownika
Wersja wielojęzykowa.
Początek obowiązywania subskrypcji wrzesień 2023 r.
Oprogramowanie do remapowania samochodów.
Identyfikacja i indeksacja tabel kalibracyjnych jednostek sterujących silnika (ECU) i jednostek sterujących skrzyń biegów (TCU).
Moduły do usuwania DTC, sum kontrolnych, natychmiastowych rozwiązań i automatycznego rozpoznawania map.
Możliwość usuwania lub modyfikowania krzywych ECU i TCU.
Wizualizację map 2D i 3D.
Automatycznie wykrywanie mapy elektroniki pojazdu (Bosch, Siemens, Delphi, Temic, Luca, Visteon, Motorola itp.)
Wymagana instalacja i konfiguracja oprogramowania na sprzęcie wskazanym przez Zamawiającego.

9. Oprogramowanie – 1 szt.	VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa):	23 %			

Subskrypcja na 12 miesięcy.
Subskrypcja oprogramowania posiadanego przez Zamawiającego pod nazwą "WAPRO Mag Prestiż Plus" (najnowsza aktualna wersja oferowana przez producenta oprogramowania z dnia składania oferty).
Początek obowiązywania subskrypcji październik 2023 r.
Wymagana instalacja i konfiguracja oprogramowania na sprzęcie wskazanym przez Zamawiającego.

10. Oprogramowanie – 800 szt.	VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa):	23 %			

Opis systemu ochrony antywirusowej z zaporą ogniową dla stacji roboczych.

Ochrona antywirusowa stacji roboczych wspiera następujące systemy operacyjne:
- Microsoft Windows 7 SP1
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows 11

Ochrona antymalware

1. Ochrona realizowana jest na wielu poziomach tj. na poziomie plików, sieci i urządzeń zewnętrznych.
2. Rozwiązanie wyposażone jest w mechanizmy do wykrywania różnego typu malware, w tym m.in. ransomware, koni trojańskich, robaków, wirusów itp.
3. Rozwiązanie wyposażone jest w silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu spyware i riskware.
4. Aktualizacje baz definicji wirusów dostępne są 24h na dobę na serwerze producenta, możliwa jest zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
5. System posiada możliwość dystrybuowania aktualizacji baz definicji wirusów, aktualizacji oprogramowania zainstalowanego na stacji końcowej oraz polityk bezpieczeństwa za pomocą serwera pośredniczącego. Serwer pośredniczący pobiera aktualizacje oprogramowania, jak i bazy antywirusowe, z serwerów producenta, a następnie dystrybuuje je w sieci lokalnej.
6. Rozwiązanie umożliwia wywołanie skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
7. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
8. Rozwiązanie pozwala na wywołania skanowania po uruchomieniu systemu operacyjnego oraz po zalogowaniu użytkownika.
9. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
10. Rozwiązanie posiada możliwość wywołania skanowania wszystkich plików, tylko określnych rozszerzeń plików

a także ich wykluczanie.
11. Rozwiązanie posiada możliwość skanowania dysków przenośnych takich jak pendrive, dyski zewnętrzne, czy dyski sieciowe.
12. Rozwiązanie pozwala na skanowanie na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
13. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
14. Rozwiązanie wykorzystuje przyrostowe (inkrementalne) pobieranie 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. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
16. Rozwiązanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
17. Rozwiązanie wykorzystuje w swoim działaniu heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
18. Rozwiązanie pozwala na wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit" oraz ataki typu 0-day.
19. Rozwiązanie wykorzystuje mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), analizujący podejrzane pliki wykonywalne.
20. Rozwiązanie pozwala na skanowanie plików skompresowanych obejmujące najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
21. Skaner antymalware pozwala na integrację z AMSI
22. Ochrona plików w czasie rzeczywistym pozwala na wykluczenie ze skanowania procesów.
23. Funkcja skanowania dysków sieciowych pozwala na skanowanie wszystkich plików, do których uzyskiwany jest dostęp lub tylko plików wykonywanych z takich zasobów.
24. Użytkownik ma możliwość uwolnienia pliku poddanego kwarantannie.
25. Uwolnienie pliku z kwarantanny odbywa się po podaniu hasła ustalonego przez administratora.
26. W przypadku wykrycia szkodliwego pliku rozwiązanie umożliwia pojęcie akcji automatycznej kwarantanny pliku, automatycznego leczenia, automatycznego usunięcia pliku, automatycznej zmiany nazwy pliku, tylko zgłoszenia infekcji lub podjęcia decyzji przez użytkownika.
27. Administrator posiada możliwość określenia reakcji silnika skanującego w odniesieniu do typu wykrytego zagrożenia.
28. Osobny typ reakcji może być określny dla malware, riskware i spyware.
29. Rozwiązanie zawiera funkcje logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów możliwy jest z poziomu GUI aplikacji.
30. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
31. Administrator ma możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.

Ochrona ruchu HTTP
1. Rozwiązanie skanuje na komputerze klienckim, dane pobierane i wysyłane przy pomocy protokołu http.
2. Administrator posiada możliwość blokowania na komputerze klienckim określonego rodzaju zawartości, nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http z witryn o nieokreślonej reputacji
3. Rozwiązanie realizuję ochronę podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
4. Rozwiązanie pozwala na graficzną informację dotycząca reputacji witryn wyświetlanych w wynikach wyszukiwania za pomocą wyszukiwarek takich jak Google, Bing.
5. Rozwiązanie zabezpiecza połączenia do witryn skategoryzowanych przez producenta jako 'bankowość elektroniczna' poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia np. z witryną banku.
6. 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.
7. Rozwiązanie posiada możliwość zablokowania uruchamiania narzędzi skryptowych i commandline podczas wyświetlania witryn określonych jako bankowość internetowa.
8. Rozwiązanie posiada możliwość usuwania zawartości schowka systemowego podczas zakończenia sesji z witrynami związanymi z bankowością online.
9. Rozwiązanie posiada możliwość blokowania narzędzi dostępu zdalnego podczas korzystania z witryn określonych jako bankowość internetowa lub określonych na liście przez administratora.

Kontrola aplikacji
1. Rozwiązanie posiada wbudowany mechanizm kontroli aplikacji.

2. Administrator ma możliwość blokowania uruchomienia aplikacji na stacji końcowej.
3. Blokowanie możliwości uruchomienia aplikacji na stacji końcowej umożliwia identyfikację aplikacji, co najmniej na podstawie identyfikatora SHA1, SHA256, nazwy pliku, nazwy produktu, wydawcy, wersji pliku.
4. Mechanizm kontroli aplikacji pozwala na kontrolę co najmniej zdarzeń takich jak, uruchamianie aplikacji, uruchamianie instalacji, uruchamianie procesu, ładowania biblioteki dynamicznej, dostępu do pliku.
5. Mechanizm kontroli aplikacji pozwala na tworzenie wielu profili i stosowania ich w zależności od potrzeb.
6. Mechanizm kontroli aplikacji pozwala na ustawienie domyślnej akcji w tym zezwolenia, zablokowania, zgłoszenia dla uruchamianych aplikacji.

Zapora sieciowa
1. Rozwiązanie posiada możliwość zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
2. Mechanizm kontroli zapory ogniowej posiada wbudowane predefiniowane profile.
3. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
4. Administrator posiada możliwość określenia domyślnej reakcji dla nieznanej komunikacji sieciowej dla ruchu przychodzącego i wychodzącego.
5. Jako domyślne akcje dla nieznanego ruchu sieciowego rozwiązanie pozwala określić blokowanie lub zezwolenie na taką komunikację.
6. Administrator posiada możliwość stworzenia reguł stosowanych w przypadku aktywacji izolacji hosta od sieci.

Kontrola www
1. Rozwiązanie posiada funkcję blokowania dostępu do kategorii witryn WWW skatalogowanych przez systemy reputacyjne producenta bez konieczności ręcznego wpisywania poszczególnych adresów.
2. Oprogramowanie zapewnia co najmniej 30 kategorii witryn WWW.
3. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
4. Rozwiązanie posiada możliwość blokowania witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.

Software updater
1. Rozwiązanie posiada wbudowany moduł aktualizacji aplikacji firm trzecich, który okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
2. Moduł aktualizacji aplikacji pełni rolę programu łatającego podatności i instalującego aktualizacje oprogramowania, a nie pasywnego skanera luk w bezpieczeństwie aplikacji.
3. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji.
4. Dodanie aplikacji wykluczonych z aktualizacji odbywa się na podstawie nazwy aplikacji, ID biuletynu oraz dostawcy aplikacji.
5. System centralnego zarządzania pozwala prezentować niezaktualizowane aplikacje na komputerach klienckich.
6. Mechanizm aktualizacji oprogramowania firm trzecich nie wymaga instalowania dodatkowych agentów oprócz agenta EPP.
7. Mechanizm aktualizacji oprogramowania firm trzecich pozwala na wymuszenie instalacji aktualizacji w sposób akcji wymuszonej z poziomu interfejsu zarządzania lub reguły harmonogramu wykonującej się w sposób zaplanowany konkretnego dnia i o konkretnej godzinie.
8. W przypadku gdy aktualizacja oprogramowania nie mogła się wykonać zgodnie z harmonogramem, zadanie instalacji może być uruchomione w najbliższym możliwym terminie z pominięciem harmonogramu.
9. W przypadku gdy aplikacja musi zostać zamknięta przed procesem aktualizacji administrator ma możliwość określenia czy ma się to odbyć automatycznie – bez wiedzy użytkownika, czy też ma się wyświetlić odpowiedni komunikat użytkownikowi z informacją o konieczności zamknięcia obecnie uruchomionej aplikacji wymagającej aktualizacji.
10. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
11. Administrator posiada możliwość skonfigurowania instalacji automatycznej aktualizacji

Kontrola nośników zewnętrznych
1. Oprogramowanie umożliwia blokowanie lub zezwalanie na dostęp do wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
2. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.
3. Rozwiązanie pozwala na nałożenie blokady zapisywania plików na zewnętrznych nośnikach pamięci (tryb tylko do odczytu).

4. Rozwiązanie pozwala na blokadę uruchamiania oprogramowania z dysków zewnętrznych, jednocześnie blokada ta umożliwia korzystanie z pozostałych danych zapisanych na takich dyskach.
5. Administrator jest informowany o podłączanych do chronionych systemów urządzeniach zewnętrznych.
6. Informacja o podłączanych urządzeniach zewnętrznych dotyczy wszystkich urządzeń lub tylko nowych.

Zaawansowana ochrona przed ransomware
1. Oprogramowanie posiada dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware.
2. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
3. Administrator posiada możliwość określenia folderów, które mają zostać objęte dodatkową ochroną przed modyfikacją.
4. Administrator posiada możliwość określenia domyślnej reakcji na próby modyfikowania plików w chronionych folderach zezwalając na taką modyfikację lub blokowanie.
5. Rozwiązanie posiada możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.

Dodatkowe funkcje
1. Instalator oprogramowania na stacji końcowej posiada możliwość sprawdzenia istnienia poprzednich wersji oprogramowania oraz oprogramowania uniemożliwiającego poprawne działanie klienta.
2. W przypadku znalezienia oprogramowania uniemożliwiającego poprawne działanie klienta, instalator informuje o tym fakcie użytkownika i w razie akceptacji pozwala usunąć takie oprogramowanie.
3. Administrator posiada możliwość zdefiniowania automatycznego procesu usuwania programowania uniemożliwiającego poprawne działanie klienta, bez informowania użytkownika końcowego.
4. Administrator posiada możliwość zablokowania deinstalacji aplikacji chroniącej przez użytkownika końcowego.
5. Deinstalacja aplikacji może odbyć się po podaniu hasła skonfigurowanego przez administratora.
6. Administrator ma możliwość granularnego zablokowania zmiany konfiguracji przez użytkownika końcowego dla poszczególnych modułów ochrony oraz dostępnych funkcji aplikacji chroniącej.

Ochrona urządzeń Mac

Ochrona antywirusowa komputerów komunikuje się z systemem centralnego zarządzania.
Oprogramowanie jest kompatybilne z następującymi systemami operacyjnymi:

- mac OS 11 Big Sur
- mac OS 10.15 Catalina
- mac OS 10.14 Mojave

1. Oprogramowanie zapewnia ochronę plików w czasie rzeczywistym, skanowania zgodnie z ustalonym harmonogramem.
2. Pozwala na tworzenie wykluczeń ze skanowania.
3. Pozwala na aktywację mechanizmu zapory ogniowej.
4. Posiada moduł ochrony przeglądania stron internetowych

Opis systemu centralnego zarządzania

System centralnego zarządzania może być zainstalowany na wersjach serwerowych systemów Microsoft Windows lub Linux.
Instalacja sytemu centralnego zarządzania dla Microsoft Windows wspiera następujące wersje systemów operacyjnych:

- Windows Server 2012 (Essentials, Standard, Datacenter)
- Windows Server 2012 R2 (Essentials, Standard, Datacenter)
- Windows Server 2016 (Essentials, Standard, Datacenter)
- Windows Server 2019 (Essentials, Standard, Datacenter)
- Windows Server 2022 (Essentials, Standard, Datacenter)

Instalacja sytemu centralnego zarządzania dla Linux wspiera następujące 64 bitowe wersje systemów operacyjnych:

- Red Hat Enterprise Linux 6,7,8
- CentOS 7, 8
- SuSE Linux Enterprise Server 11, 12, 15

• SuSE Linux Enterprise Desktop 11, 12, 15
• Debian GNU Linux 9, 10
• Ubuntu 16.04, 18.04, 20.04

1. Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej.
2. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi jest zaszyfrowana.
3. Rozwiązanie pozwala na scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta.
4. Administratorzy mają możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.
5. Centralna konsola administracyjna umożliwia przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy.
6. Rozwiązanie pozwala na tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach.
7. Rozwiązanie pozwala na import struktury drzewa z Microsoft Active Directory.
8. Rozwiązanie pozwala na tworzenie reguł synchronizacji z Microsoft Active Directory umożliwiających automatyczną synchronizację klientów z aktualnie istniejącymi grupami komputerów.
9. Rozwiązanie pozwala na tworzenie reguł powiadamiania o nowych, niezarządzanych klientach w Microsoft Active Directory.
10. Rozwiązanie pozwala na blokowanie wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników.
11. Rozwiązanie pozwala na zdefiniowania hasła do odinstalowania aplikacji.
12. Rozwiązanie pozwala na definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów.
13. Rozwiązanie posiada 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.
14. 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.
15. Rozwiązanie pozwala na konfigurację włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.
16. Rozwiązanie umożliwia administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki.
17. Rozwiązanie pozwala na eksport raportów z pracy systemu do pliku HTML.
18. Rozwiązanie daje możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich.
19. Rozwiązanie posiada dedykowany system raportowania dostępny przez przeglądarkę internetową umożliwiający podgląd statystyk dotyczących wykrytych wirusów, przeprowadzonych ataków, zainstalowanego oprogramowania oraz statystyk połączenia stacji klienckich.
20. System raportowania umożliwia wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora.
21. Zarządzanie zdarzeniami i raportowanie pozwala na 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.
22. Rozwiązanie daje możliwość przekierowania alertów bezpośrednio do serwera Syslog.
23. Rozwiązanie umożliwia tworzenie wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).
24. Rozwiązanie umożliwia wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączania programu.
25. Wykonywanie automatycznej kopii bazy danych systemu zarządzania centralnego może odbywać się zgodnie z harmonogramem określonym przez administratora.
26. Administrator posiada możliwość określenia liczby kopii bazy danych, jaka będzie przetrzymywana przez automatyczny system tworzenia kopii zapasowej.
27. Rozwiązanie posiada możliwość wygenerowania danych diagnostycznych z podpiętych komputerów za pomocą konsoli zarządzającej.
28. Rozwiązanie posiada możliwość bezpośredniego pobrania z komputera danych diagnostycznych z poziomu konsoli zarządzającej.
29. Administrator posiada możliwość komentowania stosowanej konfiguracji stacji końcowych za pomocą notatek umieszczonych w interfejsie graficznym konsoli zarządzającej.

30. Konsola wyposażona jest w panel kontrolny zawierający podstawowe informacje dotyczące obecnego stanu chronionego środowiska.
31. System zarządzania pozwala na tworzenie profili w zależności od systemu operacyjnego i wersji wykorzystywanego w organizacji oprogramowania służącego ochronie.
Wymagana instalacja i konfiguracja oprogramowania na sprzęcie wskazanym przez Zamawiającego.

11. Oprogramowanie – 25 szt.	VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa):	23 %			

Opis systemu ochrony antywirusowej z zaporą ogniową dla serwerów.

Ochrona antywirusowa serwerów wspiera następujące systemy operacyjne:
- Microsoft Small Business Server 2011, Standard edition
- Microsoft Small Business Server 2011, Essentials
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2012 R2 Foundation
- Microsoft Windows Server 2016 Standard
- Microsoft Windows Server 2016 Essentials
- Microsoft Windows Server 2016 Datacenter
- Microsoft Windows Server 2016 Core
- Microsoft Windows Server 2019 Standard
- Microsoft Windows Server 2019 Essentials
- Microsoft Windows Server 2019 Datacenter
- Microsoft Windows Server 2019 Core
- Microsoft Windows Server 2022

Dodatkowo wspierane serwery terminalowe:
- Microsoft Windows Terminal/RDP Services
- Citrix XenApp 5.0
- Citrix XenApp 6.0
- Citrix XenApp 6.5
- Citrix XenApp 7.5, 7.6, 7.14, 7.15

Ochrona antymalware
1. Ochrona realizowana jest na wielu poziomach tj. na poziomie plików, sieci i urządzeń zewnętrznych.
2. Rozwiązanie wyposażone jest w mechanizmy do wykrywania różnego typu malware, w tym m.in. ransomware, koni trojańskich, robaków, wirusów itp.
3. Rozwiązanie wyposażone jest w silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu spyware i riskware.
4. Aktualizacje baz definicji wirusów dostępne są 24h na dobę na serwerze producenta, możliwa jest zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
5. System posiada możliwość dystrybuowania aktualizacji baz definicji wirusów, aktualizacji oprogramowania zainstalowanego na stacji końcowej oraz polityk bezpieczeństwa za pomocą serwera pośredniczącego. Serwer pośredniczący pobiera aktualizacje oprogramowania, jak i bazy antywirusowe, z serwerów producenta, a następnie dystrybuuje je w sieci lokalnej.
6. Rozwiązanie umożliwia wywołanie skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
7. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
8. Rozwiązanie pozwala na wywołania skanowania po uruchomieniu systemu operacyjnego oraz po zalogowaniu użytkownika.
9. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
10. Rozwiązanie posiada możliwość wywołania skanowania wszystkich plików, tylko określnych rozszerzeń plików a także ich wykluczanie.
11. Rozwiązanie posiada możliwość skanowania dysków przenośnych takich jak pendrive, dyski zewnętrzne, czy

dyski sieciowe.
12. Rozwiązanie pozwala na skanowanie na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
13. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
14. Rozwiązanie wykorzystuje przyrostowe (inkrementalne) pobieranie 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. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
16. Rozwiązanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
17. Rozwiązanie wykorzystuje w swoim działaniu heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
18. Rozwiązanie pozwala na wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit" oraz ataki typu 0-day.
19. Rozwiązanie wykorzystuje mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), analizujący podejrzane pliki wykonywalne.
20. Rozwiązanie pozwala na skanowanie plików skompresowanych obejmujące najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
21. Skaner antymalware pozwala na integrację z AMSI
22. Ochrona plików w czasie rzeczywistym pozwala na wykluczenie ze skanowania procesów.
23. Funkcja skanowania dysków sieciowych pozwala na skanowanie wszystkich plików, do których uzyskiwany jest dostęp lub tylko plików wykonywanych z takich zasobów.
24. Użytkownik ma możliwość uwolnienia pliku poddanego kwarantannie.
25. Uwolnienie pliku z kwarantanny odbywa się po podaniu hasła ustalonego przez administratora.
26. W przypadku wykrycia szkodliwego pliku rozwiązanie umożliwia pojęcie akcji automatycznej kwarantanny pliku, automatycznego leczenia, automatycznego usunięcia pliku, automatycznej zmiany nazwy pliku, tylko zgłoszenia infekcji lub podjęcia decyzji przez użytkownika.
27. Administrator posiada możliwość określenia reakcji silnika skanującego w odniesieniu do typu wykrytego zagrożenia.
28. Osobny typ reakcji może być określny dla malware, riskware i spyware.
29. Rozwiązanie zawiera funkcje logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów możliwy jest z poziomu GUI aplikacji.
30. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
31. Administrator ma możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.

Ochrona ruchu HTTP
1. Rozwiązanie skanuje na komputerze klienckim, dane pobierane i wysyłane przy pomocy protokołu http.
2. Administrator posiada możliwość blokowania na komputerze klienckim określonego rodzaju zawartości, nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http z witryn o nieokreślonej reputacji
3. Rozwiązanie realizuję ochronę podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
4. Rozwiązanie pozwala na graficzną informację dotycząca reputacji witryn wyświetlanych w wynikach wyszukiwania za pomocą wyszukiwarek takich jak Google, Bing.
5. Rozwiązanie zabezpiecza połączenia do witryn skategoryzowanych przez producenta jako 'bankowość elektroniczna' poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia np. z witryną banku.
6. 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.
7. Rozwiązanie posiada możliwość zablokowania uruchamiania narzędzi skryptowych i commandline podczas wyświetlania witryn określonych jako bankowość internetowa.
8. Rozwiązanie posiada możliwość usuwania zawartości schowka systemowego podczas zakończenia sesji z witrynami związanymi z bankowością online.
9. Rozwiązanie posiada możliwość blokowania narzędzi dostępu zdalnego podczas korzystania z witryn określonych jako bankowość internetowa lub określonych na liście przez administratora.

Kontrola aplikacji
1. Rozwiązanie posiada wbudowany mechanizm kontroli aplikacji.
2. Administrator ma możliwość blokowania uruchomienia aplikacji na stacji końcowej.
3. Blokowanie możliwości uruchomienia aplikacji na stacji końcowej umożliwia identyfikację aplikacji, co najmniej

na podstawie identyfikatora SHA1, SHA256, nazwy pliku, nazwy produktu, wydawcy, wersji pliku.
4. Mechanizm kontroli aplikacji pozwala na kontrolę co najmniej zdarzeń takich jak, uruchamianie aplikacji, uruchamianie instalacji, uruchamianie procesu, ładowania biblioteki dynamicznej, dostępu do pliku.
5. Mechanizm kontroli aplikacji pozwala na tworzenie wielu profili i stosowania ich w zależności od potrzeb.
6. Mechanizm kontroli aplikacji pozwala na ustawienie domyślnej akcji w tym zezwolenia, zablokowania, zgłoszenia dla uruchamianych aplikacji.

Zapora sieciowa
1. Rozwiązanie posiada możliwość zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
2. Mechanizm kontroli zapory ogniowej posiada wbudowane predefiniowane profile.
3. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
4. Administrator posiada możliwość określenia domyślnej reakcji dla nieznanej komunikacji sieciowej dla ruchu przychodzącego i wychodzącego.
5. Jako domyślne akcje dla nieznanego ruchu sieciowego rozwiązanie pozwala określić blokowanie lub zezwolenie na taką komunikację.
6. Administrator posiada możliwość stworzenia reguł stosowanych w przypadku aktywacji izolacji hosta od sieci.

Kontrola www
1. Rozwiązanie posiada funkcję blokowania dostępu do kategorii witryn WWW skatalogowanych przez systemy reputacyjne producenta bez konieczności ręcznego wpisywania poszczególnych adresów.
2. Oprogramowanie zapewnia co najmniej 30 kategorii witryn WWW.
3. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
4. Rozwiązanie posiada możliwość blokowania witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.

Software updater
1. Rozwiązanie posiada wbudowany moduł aktualizacji aplikacji firm trzecich, który okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
2. Moduł aktualizacji aplikacji pełni rolę programu łatającego podatności i instalującego aktualizacje oprogramowania, a nie pasywnego skanera luk w bezpieczeństwie aplikacji.
3. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji.
4. Dodanie aplikacji wykluczonych z aktualizacji odbywa się na podstawie nazwy aplikacji, ID biuletynu oraz dostawcy aplikacji.
5. System centralnego zarządzania pozwala prezentować niezaktualizowane aplikacje na komputerach klienckich.
6. Mechanizm aktualizacji oprogramowania firm trzecich nie wymaga instalowania dodatkowych agentów oprócz agenta EPP.
7. Mechanizm aktualizacji oprogramowania firm trzecich pozwala na wymuszenie instalacji aktualizacji w sposób akcji wymuszonej z poziomu interfejsu zarządzania lub reguły harmonogramu wykonującej się w sposób zaplanowany konkretnego dnia i o konkretnej godzinie.
8. W przypadku gdy aktualizacja oprogramowania nie mogła się wykonać zgodnie z harmonogramem, zadanie instalacji może być uruchomione w najbliższym możliwym terminie z pominięciem harmonogramu.
9. W przypadku gdy aplikacja musi zostać zamknięta przed procesem aktualizacji administrator ma możliwość określenia czy ma się to odbyć automatycznie – bez wiedzy użytkownika, czy też ma się wyświetlić odpowiedni komunikat użytkownikowi z informacją o konieczności zamknięcia obecnie uruchomionej aplikacji wymagającej aktualizacji.
10. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
11. Administrator posiada możliwość skonfigurowania instalacji automatycznej aktualizacji

Kontrola nośników zewnętrznych
1. Oprogramowanie umożliwia blokowanie lub zezwalanie na dostęp do wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
2. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.
3. Rozwiązanie pozwala na nałożenie blokady zapisywania plików na zewnętrznych nośnikach pamięci (tryb tylko do odczytu).
4. Rozwiązanie pozwala na blokadę uruchamiania oprogramowania z dysków zewnętrznych, jednocześnie blokada ta umożliwia korzystanie z pozostałych danych zapisanych na takich dyskach.

5. Administrator jest informowany o podłączanych do chronionych systemów urządzeniach zewnętrznych.
6. Informacja o podłączanych urządzeniach zewnętrznych dotyczy wszystkich urządzeń lub tylko nowych.

Zaawansowana ochrona przed ransomware

1. Oprogramowanie posiada dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware.
2. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
3. Administrator posiada możliwość określenia folderów, które mają zostać objęte dodatkową ochroną przed modyfikacją.
4. Administrator posiada możliwość określenia domyślnej reakcji na próby modyfikowania plików w chronionych folderach zezwalając na taką modyfikację lub blokowanie.
5. Rozwiązanie posiada możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.

Dodatkowe funkcje

1. Instalator oprogramowania na stacji końcowej posiada możliwość sprawdzenia istnienia poprzednich wersji oprogramowania oraz oprogramowania uniemożliwiającego poprawne działanie klienta.
2. W przypadku znalezienia oprogramowania uniemożliwiającego poprawne działanie klienta, instalator informuje o tym fakcie użytkownika i w razie akceptacji pozwala usunąć takie oprogramowanie.
3. Administrator posiada możliwość zdefiniowania automatycznego procesu usuwania programowania uniemożliwiającego poprawne działanie klienta, bez informowania użytkownika końcowego.
4. Administrator posiada możliwość zablokowania deinstalacji aplikacji chroniącej przez użytkownika końcowego.
5. Deinstalacja aplikacji może odbyć się po podaniu hasła skonfigurowanego przez administratora.
6. Administrator ma możliwość granularnego zablokowania zmiany konfiguracji przez użytkownika końcowego dla poszczególnych modułów ochrony oraz dostępnych funkcji aplikacji chroniącej.

Opis systemu centralnego zarządzania

System centralnego zarządzania może być zainstalowany na wersjach serwerowych systemów Microsoft Windows lub Linux.
Instalacja sytemu centralnego zarządzania dla Microsoft Windows wspiera następujące wersje systemów operacyjnych:

- Windows Server 2012 (Essentials, Standard, Datacenter)
- Windows Server 2012 R2 (Essentials, Standard, Datacenter)
- Windows Server 2016 (Essentials, Standard, Datacenter)
- Windows Server 2019 (Essentials, Standard, Datacenter)
- Windows Server 2022 (Essentials, Standard, Datacenter)

Instalacja sytemu centralnego zarządzania dla Linux wspiera następujące 64 bitowe wersje systemów operacyjnych:

- Red Hat Enterprise Linux 6,7,8
- CentOS 7, 8
- SuSE Linux Enterprise Server 11, 12, 15
- SuSE Linux Enterprise Desktop 11, 12, 15
- Debian GNU Linux 9, 10
- Ubuntu 16.04, 18.04, 20.04

1. Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej.
2. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi jest zaszyfrowana.
3. Rozwiązanie pozwala na scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta.
4. Administratorzy mają możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.
5. Centralna konsola administracyjna umożliwia przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy.
6. Rozwiązanie pozwala na tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach.
7. Rozwiązanie pozwala na import struktury drzewa z Microsoft Active Directory.

8. Rozwiązanie pozwala na tworzenie reguł synchronizacji z Microsoft Active Directory umożliwiających automatyczną synchronizację klientów z aktualnie istniejącymi grupami komputerów.
9. Rozwiązanie pozwala na tworzenie reguł powiadamiania o nowych, niezarządzanych klientach w Microsoft Active Directory.
10. Rozwiązanie pozwala na blokowanie wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników.
11. Rozwiązanie pozwala na zdefiniowania hasła do odinstalowania aplikacji.
12. Rozwiązanie pozwala na definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów.
13. Rozwiązanie posiada 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.
14. 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.
15. Rozwiązanie pozwala na konfigurację włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.
16. Rozwiązanie umożliwia administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki.
17. Rozwiązanie pozwala na eksport raportów z pracy systemu do pliku HTML.
18. Rozwiązanie daje możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich.
19. Rozwiązanie posiada dedykowany system raportowania dostępny przez przeglądarkę internetową umożliwiający podgląd statystyk dotyczących wykrytych wirusów, przeprowadzonych ataków, zainstalowanego oprogramowania oraz statystyk połączenia stacji klienckich.
20. System raportowania umożliwia wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora.
21. Zarządzanie zdarzeniami i raportowanie pozwala na 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.
22. Rozwiązanie daje możliwość przekierowania alertów bezpośrednio do serwera Syslog.
23. Rozwiązanie umożliwia tworzenie wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).
24. Rozwiązanie umożliwia wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączania programu.
25. Wykonywanie automatycznej kopii bazy danych systemu zarządzania centralnego może odbywać się zgodnie z harmonogramem określonym przez administratora.
26. Administrator posiada możliwość określenia liczby kopii bazy danych, jaka będzie przetrzymywana przez automatyczny system tworzenia kopii zapasowej.
27. Rozwiązanie posiada możliwość wygenerowania danych diagnostycznych z podpiętych komputerów za pomocą konsoli zarządzającej.
28. Rozwiązanie posiada możliwość bezpośredniego pobrania z komputera danych diagnostycznych z poziomu konsoli zarządzającej.
29. Administrator posiada możliwość komentowania stosowanej konfiguracji stacji końcowych za pomocą notatek umieszczonych w interfejsie graficznym konsoli zarządzającej.
30. Konsola wyposażona jest w panel kontrolny zawierający podstawowe informacje dotyczące obecnego stanu chronionego środowiska.
31. System zarządzania pozwala na tworzenie profili w zależności od systemu operacyjnego i wersji wykorzystywanego w organizacji oprogramowania służącego ochronie.
Wymagana instalacja i konfiguracja oprogramowania na sprzęcie wskazanym przez Zamawiającego.

....., dnia .....
(miejscowość)

.....
podpis osoby uprawnionej
do reprezentowania Wykonawcy