załącznik nr 1 do Rozdziału III SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

L.p.	Nazwa przedmiotu zamówienia	Adres	Planowany termin realizacji usługi	UWAGI
I.	**Bitdefender GravityZone Business Security - licencja**	-	wrzesień	-
II.	**Bitdefender GravityZone Patch Management - licencja**	-	wrzesień	-

Szczegółowy opis przedmiotu zamówienia:

1. Przedmiotem zamówienia jest przedłużenie o 36 miesięcy obecnie posiadanych licencji naoprogramowanie antywirusowe Bitdefender GravityZone ważnych do 23 września 2024 roku lub równoważnych oraz zamówienie dodatkowej licencji Bitdefender GravityZone Patch Management lub równoważnej na okres 36 miesięcy, zgodnie z poniższą tabela, gdzie Zamawiający przedstawił specyfikacje techniczną:

Nr	CZĘŚĆ I - zakup licencji	
1	**Nazwa licencji: Bitdefender GravityZone Business Security lub równoważna**	
	Ilość sztuk: 90	
	Parametry	**Wartości min/ wartości max.**
	Typ licencji	odnowienie
	Okres obowiązywania	36 miesięcy
	Konsola zarządzająca	Tak, w chmurze
2	**Nazwa licencji: Bitdefender GravityZone Patch Management lub równoważna**	
	Ilość sztuk: 90	
	Parametry	**Wartości min/ wartości max.**
	Typ licencji	Nowy dodatkowy moduł do posiadanej licencji Bitdefender GravityZone Business Security lub równoważnej
	Okres obowiązywania	36 miesięcy
	Konsola zarządzająca	Tak, w chmurze

2. Wykonawca jest zobowiązany w przypadku oferowania asortymentu równoważnego przedstawić kompatybilne licencje, tak aby obie ze sobą współgrały.

3. Wykonawca dostarczy aktywne klucze licencyjne w formie elektronicznej, nie później niż w ciągu 2 dni roboczych licząc od dnia zawarcia umowy. Zgodnie z powyższym klucze winne być przekazane na poniższy adresy e-mail: k.slomka@pcinn.org.

4. Równoważność

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

1) Poprzez równoważność Zamawiający rozumie oprogramowanie, które posiada podobną/tożsamą, taką samą lub lepszą funkcjonalność, z tym że winno składać się z tożsamych aplikacji komputerowych aby w pełni zaspokoić potrzeby Zamawiającego w zakresie możliwości ochrony antywiurusowej. Zamawiający dokona oceny równoważności poprzez stwierdzenia „spełnia", „nie spełnia", dokonane na podstawie opisu równoważności oraz nazw podanych przez Wykonawcę w porównaniu z funkcjonalnością w/w aplikacji. Wszystkie aplikacje komputerowe, które zawierać będą oprogramowanie równoważne winny być tożsame lub lepsze niż aplikacje wymienione w pkt 1 powyżej oraz zapewniać pełną możliwość zabezpieczenia przy najlepszej wydajności.
2) Wykonawca oferujący przedmiot równoważny jest zobligowany podać w formularzu ofertowym nazwę licencji wraz z wskazaniem jego funkcjonalności, tak aby Zamawiający w oczywisty sposób mógł dokonać oceny równoważności.
3) W przypadku zaoferowania przez Wykonawcę Produktów równoważnych, Zamawiający ponadto wymaga, aby oferowane Produkty spełniały dodatkowo niżej wymienione wymagania:
    a) Wykonawca musi zapewnić warunki i zakres usługi wsparcia Producenta dla Produktu równoważnego nie gorsze niż usługa określona dla odpowiedniego Produktu wymienionego w pkt 1;
    b) Warunki Licencji w każdym aspekcie licencjonowania nie mogą być gorsze niż dla licencji, o których mowa w pkt 1;
    c) Wykonawca musi wykazać, że funkcjonalność Produktu równoważnego nie jest gorsza od funkcjonalności odpowiedniego Produktu, o którym mowa w pkt 1;
    d) Na żądanie Zamawiającego, Wykonawca zobowiązany jest przeszkolić pracowników Zamawiającego w zakresie funkcjonalności i działania Produktu równoważnego w terminie ustalonym z Zamawiającym, lecz nie później niż w okresie 5 dni kalendarzowych od daty zawarcia Umowy;
    e) Zamawiający wymaga, aby wszystkie aplikacje równoważne pochodziły od jednego Producenta i umożliwiały wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania i monitorowania.

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

Informacje dotyczące produktów równoważnych - warunki równoważności produktów

Licencja subskrypcyjna musi zapewnić użytkownikom co najmniej następujące możliwości:

I) Oprogramowanie zabezpieczające:

Wsparcie dla systemów operacyjnych:

- Windows 11
- Windows 10
- Windows Server 2022 Core
- Windows Server 2022
- Windows Server 2019 Core
- Windows Server 2019
- RHEL 7.x - 3.10.0 (build 957) 64-bit
- RHEL 8.x - 4.18.0 64-bit
- RHEL 9x - 5.14.0 64-bit
- CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit
- CentOS 8 Stream - 4.18.0 64-bit
- CentOS 9 Stream - 5.14.0 64-bit
- Debian 9 - 4.9.0 32-bit/64-bit
- Debian 10 - 4.19 32-bit/64-bit
- Debian 11 - 5.10 32-bit/64-bit
- Debian 12 – 6.1.0 64-bit
- Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit
- Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 6 64-bit
- Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit
- Ubuntu 22.04.x - 5.15 / 5.19 64-bit
- Ubuntu 23.04.x – 6.2.0 64-bit
- macOS Sonoma (14.x)
- macOS Ventura (13.x)
- macOS Monterey (12.x)
- macOS Big Sur (11.x)

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi
4. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżki i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog
5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6. Wbudowana technologia do ochrony przed rootkitami.
7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Ochrona krytycznych kluczy rejestru przed ich wykorzystaniem lub nieautoryzowanym dostępem do nich.
13. Możliwość dodawania wykluczeń na podstawie
    a) Plik
    b) Folder
    c) Rozszerzenie
    d) Proces
    e) Hash pliku
    f) Hash certyfikatu
    g) Nazwa zagrożenia
    h) Wiersz poleceń
    i) IP/maska

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

14. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.
15. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
16. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
17. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
18. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
19. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
20. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
21. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH
22. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
23. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
24. W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
25. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
26. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
27. Praca programu musi być niezauważalna dla użytkownika.

28. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.
29. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
30. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
31. Możliwość odblokowania ustawień programu po wpisaniu hasła
32. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu.
33. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie).
34. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu.
35. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.).
36. Funkcja Ochrony danych konfigurowana zdalnie przez administratora.
37. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
38. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
39. Wbudowany IDS.
40. Możliwość zainstalowania silnika pełnego lub lekkiego ze sprawdzaniem reputacji plików w chmurze.
41. Możliwość tworzenia list sieci zaufanych.
42. Możliwość dezaktywacji funkcji zapory sieciowej.
43. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
44. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
45. Mechanizm, który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji.

46. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa).
47. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups.
48. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.
49. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:
    a) Możliwość wymuszenia funkcji DEP systemu Windows
    b) Możliwość wymuszenia relokacji modułów (ASLR) (Systemy Windows)
50. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak:

    - Wczesny dostęp
    - Dostęp do poświadczeń
    - Wykrycie
    - Crimeware

51. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.
52. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. Formaty plików jakie mogą być odzyskane:

    3fr|ai|arw|bay|cab|cdr|cer|cr2|crt|crw|dcr|der|dgn|dll|dng|doc|docm|docx|dwg|dxf|dxg|eps|erf|exe|indd|ini|jpe|jpeg|jpg|mdf|mef|mrw|msg|msi|nef|nrw|odb|odc|odm|odp|ods|odt|orf|p12|p7b|p7c|pdd|pdf|pef|pem|pfx|png|ppt|pptm|pptx|psd|pst|ptx|py|r3d|raf|rtf|rw2|rwl|sr2|srf|srw|tsf|wb2|wpd|wps|x3f|xlk|xls|xlsb|xlsm|xlsx|xml|

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania.

53. System musi wykrywać podatne sterowniki zainstalowane na punkcie końcowym
54. Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności.
55. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows
56. System musi umożliwiać skanowanie oprogramowania układowego UEFI

Stacje robocze i serwery

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
6. Skanowanie plików spakowanych i skompresowanych.
7. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
8. Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu.
9. Produkt i sygnatury są aktualizowane nie rzadziej niż raz na godzinę.
10. Oprogramowanie posiada możliwość raportowania zdarzeń informacyjnych.
11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
12. Program musi posiadać możliwość skanowania jedynie nowych niezmienionych plików.

13. Program musi mieć wbudowany skaner wyszukiwania rootkitów.
14. Możliwość odblokowania ustawień programu po wpisaniu hasła.
15. Możliwość uruchomienia zadania skanowania z niskim priorytetem.
16. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu).
17. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
18. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem
19. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
20. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.

Konsola zarządzająca do wyboru: Cloud lub On-premise

1. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.
2. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.
3. Możliwość integracji wielu domen Active Directory
4. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
5. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
6. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi
7. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

8. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internet
9. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
10. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.
11. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
12. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv.
13. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.
14. Możliwość generowania raportu co godzinę.
15. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.
16. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
17. Możliwość dodania etykiety do stacji roboczej.
18. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
19. Możliwość przechowywania kwarantanny maksymalnie 180 dni
20. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
21. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
22. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
23. Wykorzystanie nierelacyjnej bazy danych w serwerze administracyjnym.
24. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.

25. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
26. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie
    - Zakres adresów IP/IP
    - Adres bramy
    - Adres serwera WINS
    - Adres serwera DNS
    - Połączenie DHCP sufiksów DNS
    - Punkt końcowy może rozwiązać hosta
    - Typ sieci
    - Nazwa hosta
27. Integracja z serwerem Syslog.
28. Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238
29. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.
30. Możliwość zablokowania konta w konsoli, jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.
31. Funkcja pojedynczego logowania – Single Sign-on (SSO).
32. Możliwość naprawy instalacji z poziomu konsoli.
33. Raport streszczający - Możliwość podglądu raportu, który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:
    - Zarządzane punkty końcowe
    - Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne
    - Podział zagrożeń na urządzenia takie jak stacje robocze i serwery
    - Status incydentów bezpieczeństwa, które wystąpiły
    - Stan modułów punktów końcowych
    - Ocena ryzyka firmy

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

- Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.
- Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware

34. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:

    - Pakiety
    - Sieć
    - Kwarantanna
    - Licencjonowanie
    - Integracje
    - Polityki
    - Raporty
    - Konta
    - Firmy

35. Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej, jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn, które automatycznie będą usuwane oraz pozwala na określenie godziny, kiedy te maszyny będą usuwane
36. Możliwość określenia własnego serwera NTP.
37. Integracja z vCenter Server.
38. Intergracja z Azure.
39. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
40. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
41. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS
42. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

43. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
44. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1.
45. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.
46. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Przypisywanie musi odbywać się ręcznie lub automatycznie. Musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
47. System umożliwia pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli administracyjnej.

Dla wersji cloud

Konsola Cloud – serwer administracyjny po stronie producenta

1. Ochrona krytycznych kluczy rejestru przed nieautoryzowanym dostępem lub ich wykorzystaniem.
2. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Np. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać:
   a) Funkcję, która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:
      - Ochrony przeglądarki internetowej
      - Sieć i poświadczenia
      - Błędna konfiguracja systemu operacyjnego

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.

b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.
c) System, który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.
d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.
e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.
f) System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie.

3. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.

a) Możliwość zablokowania konta w konsoli, jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.
b) Funkcja pojedynczego logowania – Single Sign-on (SSO).
c) Możliwość naprawy instalacji z poziomu konsoli.
d) Raport streszczający - Możliwość podglądu raportu, który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:
   - Zarządzane punkty końcowe
   - Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne
   - Najczęściej blokowane zagrożenia
   - Podział zagrożeń na urządzenia takie jak stacje robocze i serwery
   - Status incydentów bezpieczeństwa, które wystąpiły
   - Stan modułów punktów końcowych
   - Ocena ryzyka firmy

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

- Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.
- Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware.

4. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.

II) Oprogramowanie do zarządzania poprawkami

Wspierane systemy operacyjne

- Windows 11
- Windows 10
- Windows Server 2022
- Windows Server 2019
- CentOS 7 – GA+ (7.2003)
- macOS Big Sur (wersja 11) i nowsze.

1) Możliwość działania w trybie automatycznym
2) Możliwość oszacowania brakujących łatek
3) Możliwość zaplanowania oddzielnej automatycznej instalacji w oparciu o kategorię poprawek (bezpieczeństwo / niezwiązane z zabezpieczeniami)
4) Możliwość opóźnienia ponownego uruchomienia, jeśli instalacja łatki tego wymaga
5) Rozwiązanie musi zezwalać na tryb manualny – wykrywanie i instalacje łatek na żądanie
6) Rozwiązanie musi oferować możliwość podejrzenia wszystkich brakujących łatek ze środowiska. Informacje te zostaną zebrane w module zarządzania aktualizacjami.
7) Rozwiązanie dostarcza możliwość sprawdzenia które punkty końcowe posiadają zainstalowane lub niezainstalowane aktualizacje.

8) Rozwiązanie przesyła informacje zwrotne w przypadku niepowodzenia instalacji łatki
9) Rozwiązanie daje użytkownikowi możliwość szybkiej instalacji brakujących łatek na urządzeniu
10) Użytkownik powinien mieć możliwość dodania do czarnej listy jednej lub wielu łatek
11) Rozwiązanie raportuje brakujące łatki z perspektywy punktu końcowego (zainstalowane/ brakujące na każdym punkcie końcowym)
12) Rozwiązanie będzie okresowo wysyłać powiadomienia jeśli punkty końcowe nie posiadają zainstalowanych łatek.
13) Rozwiązanie zapewni możliwość buforowania, w ten sposób łatki będą pobierane z Internetu tylko przez niektóre przypisane punkty końcowe.
14) System wyświetla pozostały czas do automatycznego ponownego uruchomienia w powiadomieniu zarządzania poprawkami.
15) Funkcja wykrywania i informowania o każdej nowej zainstalowanej aplikacji na punkcie końcowym i dostępnych dla niej aktualizacji.
16) Możliwość automatycznego usuwania aktualizacji które nie mają już zastosowania ponieważ punkt końcowy nie istnieje lub aplikacja została usunięta.
17) Możliwość usunięcia z listy łatek które nie są już dostępne chociaż są obecne na niektórych punktach końcowych.
18) Możliwość wyszukiwania i pobierania aktualizacji dla wspieranych dystrybucji Linux i powiązanych z nimi produktów.

5. Wymagania względem Wykonawcy i przedmiotu zamówienia
   1) Oprogramowanie wymienione w niniejszym opisie przedmiotu zamówienia musi pochodzić bezpośrednio od Producenta lub z oficjalnych i autoryzowanych przez Producenta kanałów dystrybucyjnych. Zamawiający wymaga, aby Wykonawca posiadał kwalifikacje i uprawnienia wymagane do prawidłowej realizacji przedmiotu zamówienia.
   2) Zamawiający wymaga świadczenia usługi wsparcia technicznego w języku polskim przez cały okres używania Licencji Subskrypcyjnej. Usługa wsparcia technicznego świadczona będzie przez Producenta (zarówno w przypadku Produktów, o których mowa w pkt 1, jak i Produktów równoważnych)

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł

3) Zamawiający dopuszcza oferowanie Produktów o szerszym zakresie funkcjonalnym od wymaganego, zgodnie z powyższym opisem równoważności.
4) Dostarczane Produkty i świadczone usługi należące do przedmiotu zamówienia muszą spełniać postanowienia wynikające z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

Podkarpackie Centrum Innowacji Sp. z o.o.
ul. T. Lenartowicza 4, 35-051 Rzeszów
+48 507 836 617, biuro@pcinn.org, www.pcinn.org
NIP: 8133765154, REGON: 368953574, KRS: 0000710883
Sąd Rejonowy w Rzeszowie XII Wydział Gospodarczy w Rzeszowie
Kapitał Zakładowy: 500 000 zł