Nr postępowania: OR.271.107.2025

Pilchowice, dnia 25.04.2025

ZAPYTANIE OFERTOWE

na zamówienie publiczne o wartość nieprzekraczającej 80 000 złotych (netto)
W związku z realizacją Projektu Grantowego pn. „Cyberbezpieczny Samorząd - Gmina Pilchowice" w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC), Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa", Gmina Pilchowice zaprasza do złożenia oferty na dostawę licencji dla oprogramowania antywirusowego dla Urzędu Gminy Plichowice

1. **Nazwa i adres zamawiającego:**
   Gmina Pilchowice, ul. Damrota 6, 44-145 Pilchowice, NIP: 9691606890, REGON: 276257831
   Tel. 32 235 65 21, e-mail: ug@pilchowice.pl

2. **Tryb udzielenia zamówienia**

Postępowanie prowadzone jest w trybie zapytania ofertowego, zwanego dalej Zapytaniem, do którego nie mają zastosowania przepisy ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2019 r., poz. 1843 ze zm.), zwanej dalej „ustawą Pzp".

3. **Opis przedmiotu zamówienia:**

Zamawiający informuje, że przedmiotem zamówienia jest **dostawa licencji dla oprogramowania antywirusowego dla Urzędu Gminy Pilchowice** w ramach Projektu Grantowego pn. „Cyberbezpieczny Samorząd" realizowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa". Szczegółowy opis ujęto w Załączniku nr 2.

4. **Wspólny słownik zamówień:**
   48761000-0 pakiety oprogramowania antywirusowego

5. **Termin wykonania zamówienia:**

Termin I – dostawa licencji oprogramowania antywirusowego – do 7 dni roboczych od dnia podpisania umowy z Wykonawcą

6. **Informacje dotyczące ofert częściowych i wariantowych:**

Zamawiający nie dopuszcza możliwości składania ofert częściowych i wariantowych.

7. **Opis warunków udziału w postępowaniu oraz opis sposobu dokonywania oceny ich spełniania, w tym wymagane dokumenty potwierdzające spełnianie warunków:**

O udzielenie zamówienia mogą się ubiegać Wykonawcy, którzy:
- posiadają niezbędną wiedzę i doświadczenie oraz dysponują potencjałem technicznym i osobami zdolnymi do wykonania zamówienia;
- znajdują się w sytuacji ekonomicznej i finansowej i ekonomicznej zapewniającej wykonanie zamówienia;

8. **Termin otwarcia ofert i ogłoszenie wyników postępowania:**
   a. Rozpatrzenie ofert nastąpi do dnia 30.04.2025 r. do godziny 13:00 w siedzibie Zamawiającego (Urząd Gminy Pilchowice).

b. Zamawiający przyzna zamówienie temu Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w niniejszym zapytaniu i została oceniona jako najkorzystniejsza w oparciu o podane kryteria wyboru oferty.
c. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający prześle do wszystkich Wykonawców biorących udział w postępowaniu – drogą elektroniczną – Zawiadomienie o wyborze najkorzystniejszej oferty podając nazwę (firmę) albo imię i nazwisko, siedzibę albo miejsce zamieszkania i adres Wykonawcy, którego ofertę wybrano.

9. Informacje o sposobie porozumiewania się:

1. Osobą uprawnioną przez Zamawiającego do porozumiewania się z Wykonawcami jest Tomasz Bajon tel. (32) 722 79 05, e-mail: admin@pilchowice.pl .
2. We wszelkiej korespondencji kierowanej do Zamawiającego drogą elektroniczną dotyczącej niniejszego postępowania należy wskazywać numer sprawy oraz nazwę postępowania.

10. Opis przygotowania oferty:

a. Oferta winna być podpisana przez osobę upoważnioną do reprezentowania Wykonawcy w obrocie gospodarczym, zgodnie z aktem rejestracyjnym i przepisami prawa.
b. Zamawiający informuje, że oferta musi zawierać następuje informacje i dokumenty:
   - wypełniony Formularz Ofertowy stanowiący Załącznik nr 1;
c. Zamawiający informuje, że Wykonawca może złożyć wyłącznie jedną ofertę, uprzednio przygotowaną w języku polskim i sporządzoną na maszynie do pisania, komputerze lub inną trwałą i czytelną techniką oraz podpisana przez osobę(y) upoważnioną do reprezentowania Wykonawcy na zewnątrz i zaciągania zobowiązań w wysokości odpowiadającej ofercie. Podpis winien być sporządzony w sposób umożliwiający jego identyfikację, np. złożony wraz z imienną pieczątką lub czytelny (z podaniem imienia i nazwiska). Dokumenty mogą być podpisane podpisem kwalifikowanym lub profilem zaufanym.
d. Zamawiający wymaga, aby oferta została sporządzona według formularza ofertowego stanowiącego Załącznik nr 1 do zaproszenia do składania ofert.
e. Zamawiający informuje, że wszelkie poprawki lub zmiany w tekście oferty muszą być parafowane przez osobę (osoby) podpisującą ofertę i opatrzone datami ich wykonania.

11. Miejsce oraz termin składania ofert:

a. Ofertę należy złożyć osobiście w Urzędzie Gminy Pilchowice lub za pomocą poczty elektronicznej na adres email: admin@pilchowice.pl w terminie do 30.04.2025 r. do godziny 12:00 opatrzone tytułem **„Zapytanie ofertowe – Cyberbezpieczny Samorząd”**.
b. Zamawiający nie dopuszcza składania ofert częściowych.

12. Kryteria wyboru najkorzystniejszej oferty:

Za najkorzystniejszą zostanie uznana oferta spełniająca wymagania z najniższą ceną brutto za wykonanie przedmiotu zamówienia.
Kryterium: cena = 100%

13. Opis sposobu obliczenia ceny oferty:

a. Zamawiający informujące, że w sytuacji, gdy mowa jest o cenie – należy przez to rozumieć cenę w rozumieniu art. 3. ust. 1 pkt. 1 ust. 2 z dnia 9 maja 2014 r. o informowaniu o cenach towarów i usług (Dz. U. z 2019 r. poz. 178 z późniejszymi zmianami), nawet jeżeli jest płacona na rzecz osoby niebędącej przedsiębiorcą.
b. Zamawiający informuje, że podstawą obliczenia ceny ofertowej jest Formularz ofertowy stanowiący Załącznik nr 1 do niniejszego zapytania ofertowego. W odpowiednich rubrykach Wykonawcy winni przedstawić cenę netto oraz brutto za wykonanie usługi i podać wysokość stawki VAT.

c. Zamawiający informuje, że wszystkie rozliczenia między Zamawiającym, a Wykonawcą będą prowadzone w PLN.
d. Zamawiający informuje, że cena powinna uwzględniać wszelkie koszty związane z wykonaniem przedmiotu zamówienia, w tym zysk Wykonawcy.
e. Zamawiający informuje, że ceny podane przez Wykonawcę pozostaną przez cały okres realizacji przedmiotu zamówienia niezmienne.
f. Zamawiający informuje, że nie dopuszcza się zmian cen wykonania usług w okresie pomiędzy otwarciem ofert, a podpisaniem zlecenia/umowy.

14. Informacje dodatkowe:
a. Zamawiający zastrzega sobie prawo odstąpienia od zapytania na każdym jego etapie prowadzenia lub unieważnienia postępowania bez podania przyczyny.
b. Wykonawca może wprowadzić zmiany w złożonej ofercie lub ją wycofać, pod warunkiem, że uczyni to przed upływem terminu składania ofert. Zarówno zmiana, jak i wycofanie oferty wymagają zachowania formy pisemnej.
c. Zamawiający zastrzega sobie prawo podjęcia dodatkowych negocjacji w przypadku złożenia dwóch lub więcej ofert o takiej samej (najniższej) cenie.
d. Zamawiający informuje, że niniejsze postępowanie prowadzone jest na zasadach opartych na wewnętrznych uregulowaniach organizacyjnych Zamawiającego, przy jednoczesnym braku zastosowań regulacji wynikających z ustawy Prawo Zamówień Publicznych, a zapytanie nie stanowi zobowiązania Gminy Pilchowice do zawarcia umowy/zlecenia.
e. Zamawiający informuje, że zastrzega sobie możliwość do niedokonania wyboru żadnej oferty.
f. Zamawiający informuje, że jeżeli Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy/zlecenia w sprawie, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzania ich ponownego badania i oceny.
g. Zamawiający informuje, że zastrzega sobie prawo sprawdzania w toku oceny ofert wiarygodności przedstawionych przez Wykonawców dokumentów, wykazów, danych i informacji.
h. Zamawiający informuje, że niespełnienie wymagań postępowania oraz brak wymaganych dokumentów spowoduje odrzucenie oferty.
i. Zamawiający informuje, że postępowanie prowadzone jest wyłącznie w języku polskim.
j. Zamawiający informuje, że porozumiewanie się Zamawiającego z Wykonawcami odbywa się drogą pisemną z dopuszczeniem możliwości przekazywania oświadczeń, wniosków, zawiadomień i informacji za pomocą środków komunikacji elektronicznej – należy przez to rozumieć środki komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344 z późn. zm.).

15. Odrzucenie oferty
1. W niniejszym postępowaniu zostanie odrzucona oferta Wykonawcy, który:
a) złoży ofertę niezgodną z treścią niniejszego zapytania ofertowego;
b) nie spełnia warunków udziału w postępowaniu;
c) złożył ofertę po terminie składania ofert.

16. Klauzula informacyjna RODO

Klauzula informacyjna z art. 13 RODO w celu związanym z postępowaniem o udzielenie zamówienia w trybie zapytania ofertowego

Zgodnie z art. 13 ust. 1 i 2 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 oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informujemy, że:

1. Administratorem Pani/Pana danych osobowych jest Wójt Gminy Pilchowice. Wykonawca może kontaktować się z pisemnie na adres podany powyżej, telefonicznie: 32 235 65 21 lub za pomocą poczty elektronicznej: ug@pilchowice.pl;
2. Administrator- Wójt Gminy Pilchowice wyznaczyła inspektora ochrony danych, z którym może się Pani/Pan skontaktować *za pomocą poczty elektronicznej:* e-mail: nowator@nowator.edu.pl
3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu, związanym z postępowaniem o udzielenie zamówienia prowadzonym w trybie zapytania ofertowego pn." Zapytanie ofertowe – Cyberbezpieczny Samorząd";
4. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania zgodnie z przepisami prawa;
5. Pani/Pana dane osobowe będą przechowywane, przez okres 5 lat od dnia zakończenia postępowania o udzielenie zamówienia;
6. Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym związanym z przeprowadzeniem postępowania o udzielenie zamówienia, a konsekwencją niepodania danych będzie brak możliwości przystąpienia do niniejszego postępowania;
7. W odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO;
8. posiada Pani/Pan:
   - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych *;
   - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO **;
   - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa), gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
9. Nie przysługuje Pani/Panu:
   - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
   - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
   - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

* Wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.
** Wyjaśnienie: prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

Załączniki:

1) Załącznik nr 1 - Formularz ofertowy
2) Załącznik nr 2 – Szczegółowy Opis Przedmiotu Zamówienia

Zamawiający:
Gmina Pilchowice, ul. Damrota 6, 44-145 Pilchowice

Załącznik nr 1 – Formularz ofertowy
Dot. zapytania ofertowego nr OR.271.107.2025

FORMULARZ OFERTOWY:

Nazwa oferenta: ……
……
Adres oferenta: ……
……
Numer telefonu oferenta: ……
REGON oferenta: ……
NIP/PESEL oferenta: ……
Adres email oferenta: ……

W odpowiedzi na ogłoszenie w trybie zapytania ofertowego nr OR.271.107.2025 składamy niniejszą ofertę, oświadczając, że akceptuję/my w całości wszystkie warunki zawarte w zapytaniu ofertowym i oferujemy cenę:

dostawa licencji dla oprogramowania antywirusowego dla Urzędu Gminy Pilchowice w ramach Projektu Grantowego pn. „Cyberbezpieczny Samorząd" realizowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa". Szczegółowy opis ujęto w Załączniku nr 2.

Cena netto: …… złotych
Wartość VAT: …… %, co stanowi kwotę …… złotych
Cena brutto: …… złotych

Podsumowanie oferty:
Całkowita kwota netto: …… złotych (słownie: ……)
Wartość VAT: …… %, co stanowi kwotę …… złotych (słownie: ……)
Całkowita kwota brutto: …… złotych (słownie: ……)

Oświadczenia i informacje dla Oferenta:

1. Formularz ofertowy musi być podpisany przez osobę lub osoby upoważnione do reprezentowania Oferenta.

2. Oświadczam, że:
   - powyższe ceny zawierają wszystkie koszty jakie ponosi zamawiający w przypadku wyboru niniejszej oferty;
   - w cenie oferty zostały uwzględnione wszystkie koszty wykonania zamówienia;
   - akceptuję termin płatności wynoszący 14 dni.
   - zapoznałem/łam się z treścią zapytania ofertowego i nie wnoszę do niego uwag ani zastrzeżeń;
   - jeżeli nastąpią jakiekolwiek znaczne zmiany przedstawione w dokumentach załączonych do oferty, natychmiast powiadomię o nich Zamawiającego.
   - posiadam wskazane w zapytaniu ofertowym kwalifikacje zawodowe oraz doświadczenie niezbędne do wykonania przedmiotu niniejszego podstępowania.

- wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.
- podmiot, który reprezentuję nie jest powiązany powiązanym osobowo lub kapitałowo z Zamawiającym, tzn. nie występują żadne powiązania kapitałowe lub osobowe przez które rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego;
- podmiot, który reprezentuję nie podlega wykluczeniu z postępowania na podstawie art. 7 ust. 1ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

Ja, niżej podpisany/na …… wyrażam zgodę na przetwarzanie moich danych osobowych w związku z wykonywanym zamówieniem publicznym zgodnie z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz 1781).

Zamawiający:
Gmina Pilchowice, ul. Damrota 6, 44-145 Pilchowice

Załącznik nr 2 – Szczegółowy Opis Przedmiotu Zamówienia
Dot. zapytania ofertowego nr OR.271.107.2025

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA:

1/ **dostawa licencji dla oprogramowania antywirusowego dla Urzędu Gminy Pilchowice** w ramach Projektu Grantowego pn. „Cyberbezpieczny Samorząd" realizowanego w ramach Programu Operacyjnego Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Działanie 2.2. pn. „Wzmocnienie krajowego systemu cyberbezpieczeństwa".

Zamawiający wymaga przedłużenia i podniesienie obecnie wykorzystywanej licencji oprogramowania antywirusowego. Okres licencji: do 30.06.2026. Ilość licencji: **80**. Aktualnie Zamawiający korzysta z licencji na oprogramowanie ESET PROTECT ESSENTIAL i w celu zapewnienia ciągłości i rozszerzenia funkcjonalności systemu ochrony, Zamawiający określa dwa możliwe scenariusze realizacji zadania:

Scenariusz 1: Rozbudowa Licencji ESET PROTECT Entry:

Zamawiający wymaga przedłużenia i podniesienie obecnie wykorzystywanej licencji oprogramowania antywirusowego ESET PROTECT do wersji Entry na okres do 30.06.2026 r.

Zakres zamówienia obejmuje dostarczenie licencji dla 70 stanowisk wraz z podniesieniem poziomu licencji do wersji Entry.

Identyfikator publiczny obecnej subskrypcji: 3AE-HRU-JX4

Scenariusz 2: Dostarczenie Rozwiązania Równoważnego:

Zamawiający dopuszcza możliwość dostarczenia rozwiązania równoważnego, które będzie spełniać minimalne wymagania opisane poniżej. W przypadku wyboru rozwiązania równoważnego, Zamawiający wymaga dostarczenia licencji na okres do 30.06.2026 r. w ilości 70 sztuk. **W przypadku dostawy rozwiązania równoważnego – do formularza ofertowego należy dołączyć kartę produktową oferowanego rozwiązania dla możliwości weryfikacji jego funkcjonalności. Ciężar udowodnienia równoważności spoczywa na Wykonawcy.**

Wymagania Minimalne dla Rozwiązania Równoważnego:

W przypadku dostarczenia rozwiązania równoważnego, Zamawiający wymaga dodatkowo:

- Szkolenia dla Administratora: Przeprowadzenie certyfikowanego przez producenta oprogramowania szkolenia dla administratora wyznaczonego przez Urząd.
- Wdrożenie u klienta: implementacja rozwiązania w siedzibie Zamawiającego.
- Instalacja i konfiguracja: zainstalowanie oprogramowania na wyznaczonych stacjach roboczych, serwerach i urządzeniach mobilnych oraz konfiguracja systemu.
- Migracja konfiguracji: przeniesienie konfiguracji z aktualnie używanego systemu ochrony.
- Realizacja po godzinach pracy: wszystkie prace związane z wdrożeniem, instalacją i migracją muszą być przeprowadzone po godzinach pracy Urzędu, aby minimalizować potencjalne zakłócenia w pracy pracowników.

Administracja zdalna w chmurze

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych – Windows

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.

5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
- tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
- tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
- tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
- tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

• tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
• tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
• tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
• tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona stacji roboczych - macOS

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) lub nowszych.
2. Rozwiązanie musi wspierać architekturę Apple Silicon (ARM).
3. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
4. Pomoc w rozwiązaniu (help) musi być dostępna co najmniej w języku polskim oraz angielskim.
5. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
6. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
7. Rozwiązanie musi posiadać funkcjonalność, która w momencie wykrycia trybu pełnoekranowego ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań.
8. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
9. Rozwiązanie musi posiadać możliwość zdalnego zarządzania z poziomu Administracji zdalnej.
10. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

Ochrona stacji roboczych – Linux

1. Rozwiązanie musi wspierać systemy operacyjne Ubuntu Desktop, Red Hat Enterprise Linux oraz Linux Mint.
2. Rozwiązanie musi posiadać wsparcie dla dystrybucji 64-bitowych.
3. Pomoc (help) musi być dostępna co najmniej w języku polskim oraz angielskim.
4. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
5. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
6. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
7. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

8. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
9. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
10. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.

19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
   a. usunięcie zawartości urządzenia,
   b. przywrócenie urządzenie do ustawień fabrycznych,
   c. zablokowania urządzenia,
   d. uruchomienie sygnału dźwiękowego,
   e. lokalizację GPS.
6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
   a. nazwę aplikacji,
   b. nazwę pakietu,
   c. kategorię sklepu Google Play,
   d. uprawnienia aplikacji,
   e. pochodzenie aplikacji z nieznanego źródła.