Nr sprawy: **FZ-1/5614/MKO/21/FI** **Katowice, 19.11.2021 r.**

Dotyczy : Wstępnego zapytania ofertowego w celu ustalenia wartości zamówienia

Szanowni Państwo,

Zwracamy się z prośbą o wstępną ofertę na dostawę 1000 sztuk 3-letniej licencji oprogramowania antywirusowego dla stacji roboczych, serwerów plików i urządzeń mobilnych wraz z sandboxingiem w chmurze, szyfrowaniem dysków, subskrypcją wzorców wirusów i wsparciem technicznym.

WYMAGANIA OGÓLNE

Typ oferowanej licencji powinien uwzględniać status Zamawiającego – instytut badawczy podporządkowany Ministrowi Aktywów Państwowych.

Zamawiający wymaga, aby zachowana została ciągłość w ochronie antywirusowej posiadanych przez Zamawiającego stacji roboczych, serwerów plików i urządzeń mobilnych.

Zakres wsparcia technicznego:

- prawo do aktualizacji oprogramowania do nowszych wersji w trakcie obowiązywania licencji;
- wsparcie dostępne w dni robocze drogą mailową oraz telefoniczną (w godzinach od 8:00 do 18:00);
- pomoc techniczna w zakresie konfiguracji i administracji produktem oraz obejmująca rozwiązywanie typowych problemów z oprogramowaniem;
- wsparcie techniczne do oprogramowania świadczone w języku polskim, autoryzowane przez producenta oprogramowania.

Zamawiający ma obecnie 1 000 licencji ESET Protect Essential On-Prem i ESET Dynamic Threat Defense ważnych do 22.12.2021 r.

Wymóg wdrożenia oprogramowania (dotyczy sytuacji, w której Wykonawca zaoferuje inne oprogramowanie antywirusowe, niż to które obecnie posiada Zamawiający)

Wykonawca wdroży system antywirusowy u Zamawiającego. Wdrożenie obejmuje: instalację serwera/konsoli zarządzania, deinstalacja istniejących instancji oprogramowania ESET u Zamawiającego (środowisko nie jest zarządzane zdalnie, a więc nie jest w domenie), przeszkolenie personelu technicznego (max. 10 osób) w zakresie użytkowania, zarządzania oraz administrowania programem. Wdrożenie oprogramowania wraz ze szkoleniami (czas trwania szkoleń - minimum: 16h) musi być przeprowadzone maksymalnie w ciągu 4 tygodni od podpisania umowy.

Wymagana funkcjonalność oprogramowania

Wymagane oprogramowanie komputerowe:
oprogramowanie antywirusowe dla stacji roboczych, serwerów plików i urządzeń mobilnych wraz z *sandboxingiem* w chmurze, szyfrowaniem dysków, subskrypcją wzorców wirusów i wsparciem technicznym – 1 000 sztuk 3-letniej licencji.

/

Lp.	Funkcje i warunki techniczne oprogramowania komputerowego	Warunek
1	2	3
	Administracja zdalna:	
1	Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.	**Wymagane**
2	Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.	**Wymagane**
3	Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.	**Wymagane**
4	Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.	**Wymagane**
5	Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.	**Wymagane**
6	Rozwiązanie musi zapewniać utworzenie własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.	**Wymagane**
7	Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android.	**Wymagane**
8	Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie, przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.	**Wymagane**
9	Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).	**Wymagane**
10	Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.	**Wymagane**
11	Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.	**Wymagane**
12	Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.	**Wymagane**
13	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, wersję systemu operacyjnego i podzespoły komputera.	**Wymagane**

14	Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.	**Wymagane**
15	Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.	**Wymagane**
16	Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.	**Wymagane**
	Ochrona stacji roboczych:	
1	Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11).	**Wymagane**
2	Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.	**Wymagane**
3	Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.	**Wymagane**
4	Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.	**Wymagane**
5	Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	**Wymagane**
6	Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.	**Wymagane**
7	Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.	**Wymagane**
8	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.	**Wymagane**
9	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).	**Wymagane**
10	Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	**Wymagane**
11	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.	**Wymagane**
12	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.	**Wymagane**
13	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.	**Wymagane**

14	Moduł HIPS musi posiadać możliwość pracy co najmniej w pięciu trybach: • 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, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.	**Wymagane**
15	Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, zawierający co najmniej: zainstalowane aplikacje, usługi systemowe, informacje o systemie operacyjnym i sprzęcie, aktywne procesy i połączenia sieciowe, harmonogram systemu operacyjnego, pliki hosts i sterowniki. Funkcja generująca taki raport musi posiadać możliwości filtrowania.	**Wymagane**
16	Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.	**Wymagane**
17	Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).	**Wymagane**
18	Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	**Wymagane**
19	Zapora osobista rozwiązania musi pracować co najmniej w czterech trybach: • 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.	**Wymagane**
20	Rozwiązanie musi oceniać reguły zapory systemu Windows.	**Wymagane**
21	Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych.	**Wymagane**
22	Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.	**Wymagane**
23	Rozwiązanie musi posiadać możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.	**Wymagane**
24	Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.	**Wymagane**
25	Rozwiązanie musi być wyposażone w moduł bezpiecznej przeglądarki.	**Wymagane**
26	Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez użytkownika.	**Wymagane**

27	Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.	**Wymagane**
28	Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.	**Wymagane**
29	Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.	**Wymagane**
30	Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.	**Wymagane**
31	Rozwiązanie musi wykorzystywać do działania chmurę producenta.	**Wymagane**
32	Rozwiązanie musi posiadać możliwość określenia, jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu JAR, REG, MSI.	**Wymagane**
33	Administrator musi mieć możliwość zdefiniowania, po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.	**Wymagane**
34	Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.	**Wymagane**
35	Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.	**Wymagane**
36	Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.	**Wymagane**
37	Przeanalizowane pliki do analizy muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem oceniającym szkodliwość pliku.	**Wymagane**
38	W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.	**Wymagane**
39	Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć, jakie pliki zostały wysłane do analizy oraz przez kogo	**Wymagane**
40	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.	**Wymagane**
Ochrona serwera:		
1	Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux, w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux.	**Wymagane**
2	Rozwiązanie musi zabezpieczać przed wirusami, robakami i innymi zagrożeniami.	**Wymagane**
3	Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.	**Wymagane**
4	Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.	**Wymagane**
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.	**Wymagane**

6	Rozwiązanie musi wspierać automatyczną aktualizację silnika detekcji.	**Wymagane**
7	Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.	**Wymagane**
8	Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.	**Wymagane**
Dodatkowe wymagania dla ochrony serwerów Windows:		
1	Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.	**Wymagane**
2	Rozwiązanie musi posiadać system zapobiegania włamaniom na hoście (HIPS).	**Wymagane**
3	Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	**Wymagane**
4	Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.	**Wymagane**
5	Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.	**Wymagane**
6	Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.	**Wymagane**
7	Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.	**Wymagane**
8	Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.	**Wymagane**
Dodatkowe wymagania dla ochrony serwerów Linux:		
1	Rozwiązanie musi pozwalać na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.	**Wymagane**
2	Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.	**Wymagane**
3	Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.	**Wymagane**
4	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.	**Wymagane**
Szyfrowanie:		
1	System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10/11 32-bit i 64-bit.	**Wymagane**
2	System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).	**Wymagane**
3	Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.	**Wymagane**

4	Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.	**Wymagane**
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.	**Wymagane**
2	Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.	**Wymagane**
3	Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności.	**Wymagane**
4	Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.	**Wymagane**
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.	**Wymagane**
6	Rozwiązanie musi zapewniać administratorowi podejrzenie zainstalowanych aplikacji.	**Wymagane**
7	Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o nazwę pakietu/aplikacji.	**Wymagane**
Wymagania systemowe:		
1	Pełne wsparcie dla systemów MS Windows 7 / 8 / 10 /11.	**Wymagane**
2	Wykorzystywanie wcześniejszych wersji oprogramowania w trybie *downgrade* dla starszych systemów operacyjnych.	**Wymagane**
3	Wsparcie dla 32-bitowej i 64-bitowej wersji systemu MS Windows	**Wymagane**
4	Wersja programu dla stacji roboczych MS Windows musi być dostępna zarówno w języku polskim, jak i angielskim.	**Wymagane**
5	Pomoc (ang. *help*) i dokumentacja do programu dostępne w języku polskim.	**Wymagane**

Należy podać:

- **Cenę netto w PLN / brutto w PLN (cena winna obejmować koszty opakowania, transportu i ubezpieczenia od Wykonawcy do Zamawiającego) oraz stawkę i wartość podatku VAT,**
- **Wykonawca zobowiązany jest do złożenia oferty wstępnej na załączniku nr 1 do niniejszego wstępnego zapytania oraz wypełnienia wszystkich pól kolumny nr 4 formularza ofertowego. Wykonawca zobowiązany jest również do podania pełnej nazwy oprogramowania.**

Miejsce i termin składania ofert wstępnych:

Wstępną ofertę należy złożyć do dnia **24.11.2021. do godziny 14:00** drogą elektroniczną lub w siedzibie Zamawiającego:

Główny Instytut Górnictwa
Dział Handlowy (FZ-1)
Plac Gwarków 1
40-166 Katowice

adres e-mail: makolczyk@gig.eu

Kontakt handlowy:

mgr inż. Marzena Kolczyk - tel. (32) 259 23 42, e-mail: **makolczyk@gig.eu**

ZAPRASZAMY DO SKŁADANIA OFERT

Z poważaniem,

Kierownik Działu Handlowego

mgr Monika Wallenburg

Załącznik nr 1

Wstępna oferta na dostawę Dostawa 1000 sztuk 3-letniej licencji oprogramowania antywirusowego dla stacji roboczych, serwerów plików i urządzeń mobilnych wraz z sandboxingiem w chmurze, szyfrowaniem dysków, subskrypcją wzorców wirusów i wsparciem technicznym.

Nazwa/Imię i Nazwisko Wykonawcy:
.....
Adres: .....
Nr tel.: .....
Adres e-mail: .....
Osoba do kontaktu: .....

Oferujemy wykonanie przedmiotu zamówienia zgodnie z warunkami zawartymi we wstępnym zapytaniu ofertowym za cenę:

Lp.	Należy podać pełną nazwę zaoferowanego oprogramowania	Jednostka miary	Ilość	Cena jedn. (netto) w PLN	Wartość ogółem (netto) w PLN	Stawka (%) podatku VAT	Kwota podatku VAT w PLN	Wartość ogółem (brutto) w PLN
1	2	3	4	5	6	7	8	9
1		szt.	1000					
RAZEM :								

Wykonawca zobowiązany jest do wypełnienia wszystkich pól kolumny nr 4 poniższej tabeli „Wymagania funkcjonalność oprogramowania". Wykonawca zobowiązany jest również do podania pełnej nazwy oprogramowania.

Wymagana funkcjonalność oprogramowania

Niniejszym oferujemy dostawę oprogramowania spełniającego poniższe wymagania techniczne:	
Wymagane oprogramowanie komputerowe: oprogramowanie antywirusowe dla stacji roboczych, serwerów plików i urządzeń mobilnych wraz z *sandboxingiem* w chmurze, szyfrowaniem dysków, subskrypcją wzorców wirusów i wsparciem technicznym – 1 000 sztuk 3-letniej licencji.	**Oferowane oprogramowanie komputerowe:** .... **/należy podać pełną nazwę oprogramowania/**

Lp.	Funkcje i warunki techniczne oprogramowania komputerowego	Warunek	Informacja w zakresie spełnienia warunków. Proszę wypełnić wiersze poprzez wpisanie TAK lub NIE
1	2	3	4
	Administracja zdalna:		
1	Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.	**Wymagane**	
2	Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.	**Wymagane**	
3	Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.	**Wymagane**	
4	Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.	**Wymagane**	
5	Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.	**Wymagane**	
6	Rozwiązanie musi zapewniać utworzenie własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.	**Wymagane**	
7	Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android.	**Wymagane**	
8	Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie, przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.	**Wymagane**	
9	Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).	**Wymagane**	
10	Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.	**Wymagane**	
11	Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.	**Wymagane**	
12	Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.	**Wymagane**	
13	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, wersję systemu operacyjnego i podzespoły komputera.	**Wymagane**	
14	Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.	**Wymagane**	
15	Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.	**Wymagane**	
16	Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.	**Wymagane**	
	Ochrona stacji roboczych:		
1	Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11).	**Wymagane**	
2	Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.	**Wymagane**	

3	Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.	**Wymagane**	
4	Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.	**Wymagane**	
5	Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	**Wymagane**	
6	Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.	**Wymagane**	
7	Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.	**Wymagane**	
8	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.	**Wymagane**	
9	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).	**Wymagane**	
10	Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	**Wymagane**	
11	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.	**Wymagane**	
12	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.	**Wymagane**	
13	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.	**Wymagane**	
14	Moduł HIPS musi posiadać możliwość pracy co najmniej w pięciu trybach: • 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, • tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.	**Wymagane**	
15	Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, zawierający co najmniej: zainstalowane aplikacje, usługi systemowe, informacje o systemie operacyjnym i sprzęcie, aktywne procesy i połączenia sieciowe, harmonogram systemu operacyjnego, pliki hosts i sterowniki. Funkcja generująca taki raport musi posiadać możliwości filtrowania.	**Wymagane**	
16	Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.	**Wymagane**	
17	Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).	**Wymagane**	
18	Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	**Wymagane**	
19	Zapora osobista rozwiązania musi pracować co najmniej w czterech trybach:	**Wymagane**	

	• 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.		
20	Rozwiązanie musi oceniać reguły zapory systemu Windows.	**Wymagane**	
21	Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych.	**Wymagane**	
22	Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.	**Wymagane**	
23	Rozwiązanie musi posiadać możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.	**Wymagane**	
24	Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.	**Wymagane**	
25	Rozwiązanie musi być wyposażone w moduł bezpiecznej przeglądarki.	**Wymagane**	
26	Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez użytkownika.	**Wymagane**	
27	Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.	**Wymagane**	
28	Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.	**Wymagane**	
29	Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.	**Wymagane**	
30	Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.	**Wymagane**	
31	Rozwiązanie musi wykorzystywać do działania chmurę producenta.	**Wymagane**	
32	Rozwiązanie musi posiadać możliwość określenia, jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu JAR, REG, MSI.	**Wymagane**	
33	Administrator musi mieć możliwość zdefiniowania, po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.	**Wymagane**	
34	Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.	**Wymagane**	
35	Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.	**Wymagane**	
36	Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.	**Wymagane**	
37	Przeanalizowane pliki do analizy muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem oceniającym szkodliwość pliku.	**Wymagane**	
38	W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.	**Wymagane**	
39	Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć, jakie pliki zostały wysłane do analizy oraz przez kogo	**Wymagane**	
40	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.	**Wymagane**	
	Ochrona serwera:		
1	Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux, w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux oraz Amazon Linux.	**Wymagane**	
2	Rozwiązanie musi zabezpieczać przed wirusami, robakami i innymi zagrożeniami.	**Wymagane**	
3	Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.	**Wymagane**	

4	Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.	**Wymagane**	
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.	**Wymagane**	
6	Rozwiązanie musi wspierać automatyczną aktualizację silnika detekcji.	**Wymagane**	
7	Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.	**Wymagane**	
8	Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.	**Wymagane**	
	Dodatkowe wymagania dla ochrony serwerów Windows:		
1	Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.	**Wymagane**	
2	Rozwiązanie musi posiadać system zapobiegania włamaniom na hoście (HIPS).	**Wymagane**	
3	Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	**Wymagane**	
4	Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.	**Wymagane**	
5	Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.	**Wymagane**	
6	Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.	**Wymagane**	
7	Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.	**Wymagane**	
8	Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.	**Wymagane**	
	Dodatkowe wymagania dla ochrony serwerów Linux:		
1	Rozwiązanie musi pozwalać na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.	**Wymagane**	
2	Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.	**Wymagane**	
3	Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.	**Wymagane**	
4	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.	**Wymagane**	
	Szyfrowanie:		
1	System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10/11 32-bit i 64-bit.	**Wymagane**	
2	System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).	**Wymagane**	
3	Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.	**Wymagane**	
4	Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.	**Wymagane**	
	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.	**Wymagane**	

2	Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.	**Wymagane**	
3	Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności.	**Wymagane**	
4	Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.	**Wymagane**	
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.	**Wymagane**	
6	Rozwiązanie musi zapewniać administratorowi podejrzenie zainstalowanych aplikacji.	**Wymagane**	
7	Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o nazwę pakietu/aplikacji.	**Wymagane**	
Wymagania systemowe:			
1	Pełne wsparcie dla systemów MS Windows 7 / 8 / 10 /11.	**Wymagane**	
2	Wykorzystywanie wcześniejszych wersji oprogramowania w trybie *downgrade* dla starszych systemów operacyjnych.	**Wymagane**	
3	Wsparcie dla 32-bitowej i 64-bitowej wersji systemu MS Windows	**Wymagane**	
4	Wersja programu dla stacji roboczych MS Windows musi być dostępna zarówno w języku polskim, jak i angielskim.	**Wymagane**	
5	Pomoc (ang. *help*) i dokumentacja do programu dostępne w języku polskim.	**Wymagane**	

Przyjmujemy do wiadomości, że niewypełnienie pozycji określonych w kolumnie 4 lub udzielenie odpowiedzi negatywnej „NIE" spowoduje odrzucenie oferty.

OŚWIADCZENIE RODO DLA WYKONAWCY

1. 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", informuję, że:

- administratorem danych osobowych **WYKONAWCY** jest: *Główny Instytut Górnictwa, Plac Gwarków 1,40 - 166 Katowice,*
- inspektorem ochrony danych osobowych w *Głównym Instytucie Górnictwa* jest Pani: *mgr Katarzyna Kareł, e-mail: gdpr@gig.eu.*
- dane osobowe **WYKONAWCY** przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym wstępnym zapytaniem ofertowym,
- odbiorcami danych osobowych **WYKONAWCY** będą osoby lub podmioty, którym udostępniona zostanie dokumentacja dotycząca niniejszego wstępnego zapytania ofertowego,
- dane osobowe **WYKONAWCY** będą przechowywane przez okres 4 lat,
- w odniesieniu do danych osobowych **WYKONAWCY** decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- **WYKONAWCA** posiada :
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych dotyczących **WYKONAWCY** ;
  - na podstawie art. 16 RODO prawo do sprostowania danych osobowych **WYKONAWCY** ;
  - 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, gdy **WYKONAWCA** uzna, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- **WYKONAWCY** nie przysługuje:
  - 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 danych osobowych WYKONAWCY jest art. 6 ust. 1 lit. c RODO.**

....

Miejscowość, data *Podpis*