**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI III**

|  |  |
| --- | --- |
| **L.p.** | **Parametry wymagane** |
| 1. **Dostawa licencji dotyczących aktualizacji oprogramowania antywirusowego ESET Protect Essential Plus On-Prem lub oprogramowanie równoważne – 751 szt.\***
 |
| 1 | **Zakres zamówienia.**Przedmiot zamówienia obejmuje odnowienie na okres 1 roku (licząc od dnia 19.12.2023 r.) posiadanych przez zamawiającego licencji dla ochrony 751 stacji roboczych oraz serwerów plików (aktualizacja oprogramowania antywirusowego) z rozszerzoną funkcjonalnością Plus, On-Prem i bazy danych sygnatur wirusów oprogramowania obecnie eksploatowanego w Warmińsko-Mazurskim Urzędzie Wojewódzkim w Olsztynie, Delegaturach Urzędu w Elblągu i Ełku oraz na przejściach granicznych: Grzechotki, Bezledy, Gronowo, Gołdap, Braniewo, Elbląg ESET Protect Essential Plus On-Prem w sieci komputerowej wraz z konsolą do zarządzania dla kompleksowej ochrony systemów komputerowych.  |
| 2 | **Równoważność oprogramowania antywirusowego** **w stosunku do oprogramowania określonego w specyfikacji warunków zamówienia**.Przez równoważność oprogramowania należy rozumieć spełnienie następujących wymagań:1. oferowane oprogramowanie musi spełniać wymagania określone w punkcie 3 zawierającym specyfikację wymagań funkcjonalnych,
2. wykonawca wdroży oprogramowanie równoważne w terminie wskazanym w specyfikacji warunków zamówienia, przy czym okres od deinstalacji dotychczas funkcjonującego oprogramowania do wdrożenia zaproponowanego oprogramowania równoważnego nie może być dłuższy niż 3 dni robocze. Czynności muszą być wykonywane w godzinach pracy zamawiającego tj. od godz. 7:30 do godz. 15:30, od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy,
3. wykonawca przeszkoli personel techniczny (6 osób) w zakresie używania, zarządzania oraz administrowania programem,
4. wykonawca przygotuje i przekaże zamawiającemu wersję elektroniczną instrukcji obsługi interfejsu użytkownika oprogramowania zainstalowanego na komputerze,
5. wykonawca dokona pełnego odinstalowania istniejącego oprogramowania w liczbie 751 licencji w następujących lokalizacjach: Olsztyn (trzy lokalizacje), Elbląg, Ełk, Grzechotki, Bezledy, Gronowo, Braniewo, Gołdap, łącznie z usunięciem wpisów w rejestrach systemowych,
6. wykonawca dokona zainstalowania oprogramowania na komputerach w liczbie zgodnej z liczbą wymaganych licencji.
 |
| 3 | 1. **Centralne zarządzanie:**
2. 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,
3. rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL lub MySQL wraz z licencją, jeśli oprogramowanie antywirusowe tego wymaga,
4. rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta,
5. rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL,
6. rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów,
7. rozwiązanie musi zapewniać utworzenie własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów,
8. rozwiązanie musi wspierać zarządzanie urządzeniami mobilnymi z systemem iOS i Android,
9. rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci,
10. 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),
11. rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT,
12. rozwiązanie musi zapewniać wymuszenia dwuskładnikowej autoryzacji podczas logowania do konsoli administracyjnej,
13. rozwiązanie musi zapewniać tworzenie grup statycznych i dynamicznych komputerów. 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,
14. rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora,
15. rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog,
16. rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami,
17. rozwiązanie musi posiadać możliwość włączenia oraz skonfigurowania automatycznych aktualizacji oprogramowania antywirusowego na urządzeniach klienckich. Automatyczna aktualizacja, jeśli dotyczy, musi obejmować wszystkie komponenty oprogramowania antywirusowego,
18. rozwiązanie automatycznych aktualizacji musi mieć możliwość ograniczenia działania do wybranych wersji przez administratora.
19. **Ochrona stacji roboczych:**
20. rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10), LINUX oraz MacOS (10.12 lub nowsze),
21. rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor,
22. rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet,
23. rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji,
24. rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików,
25. rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu,
26. rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych,
27. 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,
28. 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),
29. rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS,
30. 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 zapewniać możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie,
31. 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,
32. 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,
33. rozwiązanie musi posiadać system zapobiegania włamaniom pracujący w jednym z pięciu trybów:
	1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
	2. tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
	3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
	4. tryb uczenia się, w którym program 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,
	5. tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach,
34. rozwiązanie musi posiadać wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, 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,
35. rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji,
36. rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne),
37. rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego,
38. rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day wykorzystujące działanie chmury producenta,
39. rozwiązanie musi posiadać możliwość wstrzymania otwarcia pliku przez użytkownika przed wykonaniem analizy,
40. 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,
41. rozwiązanie musi posiadać opcję zdefiniowania po jakim czasie przesłane pliki zostaną usunięte z serwerów producenta,
42. rozwiązanie musi posiadać możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek,
43. rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania,
44. rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione,
45. rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych,
46. rozwiązanie musi zapewniać odpowiednie oznaczenie dla przeanalizowanych próbek. Analiza pliku może zakończyć się z wynikiem w minimum czterostopniowej skali:
	1. czysty,
	2. podejrzany,
	3. bardzo podejrzany,
	4. szkodliwy.
47. **Ochrona serwera plików:**
48. rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowsze,
49. rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami,
50. rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor,
51. rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami i exploitami,
52. system antywirusowy musi wspierać wykorzystywanie wielu wątków skanowania w przypadku maszyn wieloprocesorowych,
53. rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście,
54. rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS,
55. 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,
56. rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki,
57. rozwiązanie musi posiadać możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line),
58. 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 zapewniać możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie,
59. rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji,
60. rozwiązanie musi wspierać skanowanie magazynu Hyper-V,
61. rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów,
62. rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego,
63. rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych,
64. rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP,
65. rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup,
66. rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty,
67. rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
 |

|  |  |
| --- | --- |
| **L.p.** | **Parametry wymagane** |
| 1. **Dostawa nowych licencji oprogramowania antywirusowego ESET Protect Essential Plus On-Prem lub oprogramowanie równoważne – 15 szt.\***
 |
| 1 | **Zakres zamówienia.**Przedmiot zamówienia obejmuje dostawę nowych (dodatkowych do już posiadanych) 15 szt. licencji oprogramowania antywirusowego ESET Protect Essential Plus On-Prem wraz z konsolą do zarządzania dla kompleksowej ochrony systemów komputerowych oraz aktualizacją bazy danych sygnatur wirusów oprogramowania do posiadanych i użytkowanych już przez zamawiającego. Zamawiający dopuszcza możliwość zaoferowania oprogramowania równoważnego na następujących zasadach:1. oprogramowanie równoważne będzie spełniało wymagania określone w tabeli nr 1 pkt 2 (Równoważność oprogramowania antywirusowego w stosunku do oprogramowania określonego w specyfikacji warunków zamówienia),
2. wykonawca wskaże zaoferowane oprogramowanie w tabeli znajdującej się w pkt 3 formularza oferty – załącznika nr 1 do specyfikacji warunków zamówienia.
 |

\* zamawiający wymaga, aby wykonawca zaoferował licencje oprogramowania, o których mowa w pkt 1 i 2 tabeli **tego samego producenta**.