OPIS PRZEDMIOTU ZAMÓWIENIA

1. Część I Dostawa urządzenia NAS RACK 19” 1 szt.

Kieszenie na dyski – min. 12 szt. 3,5"

Obsługa dysków – min.: 3,5” SATA, 2,5” SATA, 2,5” SSD SATA (wymiana dysków przy włączonym zasilaniu)

RAID – min.: 0, 1, 5, 6, 10, 50, 60, JBOD, Single Disk

Rodzaje wyjść / wejść - min.: USB 3.0 - 4 szt., RJ-45 100/1000 (LAN) - 2 szt., PCIe Gen2 (x2) - 1 szt.

Procesor - min. 4 rdzenie, 1.7 GHz

Pamięć RAM - min. 4 GB (DDR4) ( z możliwością rozbudowy do min. 16 GB)

Obsługa przez oprogramowanie systemowe NAS kopii migawkowej na poziomie bloków, z możliwością zagwarantowania miejsca na migawki

Dodatkowe informacje - obsługa przechowywania kopii zapasowych w chmurze

Wysokość – max. 2U, możliwość montażu w szafie RACK 19”,

Zasilanie –min. 250 W x2 (redundantne zasilanie)

Dołączone akcesoria – min.: kabel sieciowy, kable zasilania, elementy potrzebne do montażu NAS-a w szafie RACK,

Dyski – 6 szt. o pojemności min. 6 TB każdy dedykowane do pracy z urządzeniami typu NAS

Gwarancja – min. 24 miesiące

W przypadku urządzenia NAS dyski na czas naprawy urządzenia jak również w przypadku ich uszkodzenia muszą pozostać u Zamawiającego.

1. Część II Dostawa Kabli

Kabel żelowany FTPw kat.6 F/UTP – 50m

Kabel teleinformatyczny U/UTP kat.6 - /305m/ - 1 rolka

Patchcord UTP kat.6 zielony 1m – 5 szt.

Patchcord UTP kat.6 czerwony 2m – 3szt.

Patchcord UTP kat.6 zielony 0,5m – 5szt.

Patchcord UTP Kat. 6 fioletowy 2m – 3szt.

1. Część III Dostawa oprogramowania Office LTSC Professional Plus 2021

Office LTSC Professional Plus 2021 - 4 szt.

Zamawiający nie jest uprawniony do korzystania z wersji oprogramowania GOV, EDU oraz wersji dla użytkowników domowych i studentów.

Licencje dożywotnie

1. Część IV Dostawa licencji na urządzenie STORMSHIELD SN 510

Premium UTM Security Pack (UTM Security Pack + Zaawansowany Antywirus + Audyt Podatności + Rozszerzony filtr URL) na 3 lata – 1 licencja

Obecna licencja wygasa 10.09.2022

1. Część V Dostawa licencji na oprogramowanie antywirusowe

Przedmiotem zmówienia jest zakup licencji na oprogramowanie antywirusowe jako migracja z obecnie posiadanego oprogramowania antywirusowego Kaspersky Endpoint Security for Windows w wersji Advanced dla 150 licencji **(licencja wygasa w dniu 11.07.2024)** , w tym 8 licencji na serwer na okres 36 miesięcy. Oprogramowanie musi posiadać następujące funkcje:

Użyte w opisie określenia opisują funkcjonalności, a nie konkretny produkt. Każdy produkt realizujący równoważne funkcje spełnia warunki.

# I. Oprogramowanie Antywirusowe na stacje robocze

1. Program musi wspierać następujące platformy:
	* Windows 11 Home / Pro / Education / Enterprise
	* Windows 10 Home / Pro / Education / Enterprise
	* Windows 8.1 Professional / Enterprise
	* Windows 8 Professional / Enterprise
	* Windows 7 Home / Professional / Enterprise Service Pack 1 lub nowszy
2. Program musi umożliwić działanie na sprzęcie o minimalnych parametrach sprzętowych:
	* Procesor 1 GHz lub szybszy (wymagana jest obsługa SSE2).
	* Pamięć RAM:
		+ 1 GB dla 32-bitowych systemów operacyjnych.
		+ 2 GB dla 64-bitowych systemów operacyjnych.
	* 2 GB wolnej przestrzeni na dysku twardym.
3. Polskojęzyczny interfejs konsoli programu i jego monitora na stacjach roboczych.
4. Program powinien posiadać certyfikaty niezależnych laboratoriów.
5. Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.
6. Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń
7. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
8. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji
9. Program ma posiadać dedykowany moduł blokujący określone kategorie urządzeń (min. pamięci masowe, CD-ROM).
10. Możliwość tworzenia reguł blokujących/zezwalających na korzystanie z danego urządzenia w zależności od konta, na którym pracuje użytkownik.
11. Możliwość utworzenia listy zaufanych urządzeń na podstawie wykrytych urządzeń, bądź identyfikatora urządzenia dla określonego konta użytkownika systemu Windows.
12. Program powinien zawierać moduł wykorzystujący zestaw reguł do śledzenia nietypowych zachować na chronionych komputerach.
13. Reguły powinny być aktualizowane.
14. Moduł powinien posiadać możliwość tworzenia wykluczeń dla poszczególnych reguł.
15. Ochrona przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem (w tym Java i ActiveX).
16. Wbudowany moduł chroniący pamięć procesów systemowych
17. Możliwość wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hakerskich.
18. Wbudowany moduł skanujący i oczyszczający protokoły POP3, SMTP, IMAP niezależnie od klienta pocztowego.
19. Wbudowany moduł skanujący ruch HTTP w czasie rzeczywistym niezależnie od przeglądarki.
20. Wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa.
21. Wbudowany moduł kontrolujący dostęp do rejestru systemowego.
22. Wbudowany moduł chroniący przed phishingiem.
23. Ochrona przed niebezpiecznymi rodzajami aktywności sieciowej i atakami, możliwość tworzenia reguł wykluczających dla określonych adresów/zakresów IP.
24. Kontrola systemu poprzez ochronę proaktywną przed nowymi zagrożeniami, które nie znajdują się w antywirusowych bazach danych takimi jak np.:
* Ukierunkowane ataki
* Podejrzane pliki i ruch w sieci
* Exploity
* Grayware
1. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym, w tym zabezpieczenie udostępnionych zasobów przed zewnętrznym szyfrowaniem.
2. Moduł ochrony proaktywnej musi działać w trybach które administrator może dowolnie zmieniać na:
	* Tolerancyjny
	* Normalny
	* Agresywny
3. Centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym.
4. System antywirusowy ma posiadać możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia.
5. Leczenie i usuwanie plików co najmniej z archiwów następujących formatów 7z, RAR, ZIP, CAB.
6. Terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur.
7. Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
8. Możliwość tworzenia list zaufanych procesów, dla których aktywność nie będzie monitorowana.
9. Program ma posiadać możliwość zresetowania wszystkich ustawień włącznie z regułami stworzonymi przez użytkownika.
10. Program musi posiadać możliwość zablokowania operacji zamykania programu, zatrzymywania zadań, wyłączania ochrony, wyłączania profilu administracyjnego, zmiany ustawień, usunięcia licencji przy użyciu zdefiniowanego hasła.
11. Skanowanie w czasie rzeczywistym:
	* Uruchamianych, otwieranych, kopiowanych, przenoszonych lub tworzonych plików.
	* Pobieranej i wysyłanej z Internetu poczty elektronicznej (wraz z załącznikami) po protokołach POP3, SMTP, IMAP niezależnie od klienta pocztowego.
	* Plików pobieranych z Internetu po protokole HTTP.
	* Poczty elektronicznej przetwarzanej przez program MS Outlook niezależnie od wykorzystywanego protokołu pocztowego.
12. W przypadku wykrycia wirusa monitor antywirusowy winien automatycznie:
	* Podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe usuwać obiekt. Przed usunięciem zainfekowanego obiektu monitor antywirusowy powinien przenieść go w bezpieczny obszar dysku – kwarantanna, plik w kwarantannie powinien być zaszyfrowany.
	* Rejestrować w pliku raportu informację o wykryciu wirusa
	* Powiadamiać administratora przy użyciu poczty elektronicznej
13. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie”.
14. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
15. Możliwość skanowania dysków sieciowych i dysków przenośnych
16. Program powinien posiadać możliwość określenia harmonogramu pobierania uaktualnień, w tym możliwość wyłączenia aktualizacji automatycznej.
17. Program powinien posiadać możliwość określenia źródła uaktualnień.
18. Program musi posiadać możliwość określenia ustawień serwera proxy w przypadku, gdy jest on wymagany do nawiązania połączenia z Internetem.
19. Program powinien posiadać możliwość określenia okresu przechowywania raportów.
20. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.

# II. Oprogramowanie Antywirusowe na serwer

1. Program musi wspierać następujące platformy:
	* Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
	* Windows Server 2016 Essentials / Core / Standard / Datacenter;
	* Windows Server 2019 Essentials / Core / Standard / Datacenter.
	* Windows Server 2022 Essentials / Standard / Datacenter.
2. Program musi spełniać następujące minimalne wymagania sprzętowe:

Procesor 1 GHz lub szybszy (wymagana jest obsługa SSE2).

* + Pamięć RAM:

1 GB dla 32-bitowych systemów operacyjnych.

2 GB dla 64-bitowych systemów operacyjnych.

* + 2 GB wolnej przestrzeni na dysku twardym.
1. Polskojęzyczny interfejs konsoli programu i jego monitora.
2. Program powinien posiadać certyfikaty niezależnych laboratoriów.
3. Program powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hakerskich, oprogramowania typu spyware i adware, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.
4. Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony.
5. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
6. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji
7. Wbudowany moduł zapobiegający wykorzystaniu luk w aplikacjach zainstalowanych na stacji roboczej oraz w samym systemie operacyjnym.
8. Wbudowany moduł chroniący pamięć procesów systemowych
9. Ochrona przed niebezpiecznymi rodzajami aktywności sieciowej i atakami, możliwość tworzenia reguł wykluczających dla określonych adresów/zakresów IP.
10. Kontrola systemu poprzez ochronę proaktywną przed nowymi zagrożeniami, które nie znajdują się w antywirusowych bazach danych takimi jak np.:
* Ukierunkowane ataki
* Podejrzane pliki i ruch w sieci
* Exploity
* Grayware
1. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym.
2. Wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa.
3. Centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym.
4. System antywirusowy ma posiadać możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia.
5. Leczenie i usuwanie plików co najmniej z archiwów następujących formatów 7z, RAR, ZIP, CAB.
6. Możliwość zablokowania dostępu do ustawień programu dla użytkowników nie posiadających uprawnień administracyjnych.
7. Terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur.
8. Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
9. Możliwość tworzenia list zaufanych procesów, dla których nie będzie monitorowana aktywność.
10. Predefiniowane zestawy reguł monitorowania dla typowych aplikacji serwerowych np. Serwer MSSQL, mySQL, IIS itp.
11. Możliwość dynamicznej zmiany użycia zasobów systemowych w zależności od obciążenia systemu przez aplikacje użytkownika.
12. Program posiada funkcję chroniącą pliki, foldery i klucze rejestru wykorzystywane przez program przed zapisem i modyfikacją.
13. Program ma posiadać możliwość zresetowania wszystkich ustawień włącznie z regułami stworzonymi przez użytkownika.
14. Program musi posiadać możliwość zablokowania operacji zamykania programu, zatrzymywania zadań, wyłączania ochrony, wyłączania profilu administracyjnego, zmiany ustawień, usunięcia licencji przy użyciu hasła.
15. W przypadku wykrycia wirusa monitor antywirusowy powinien automatycznie:
* Podejmować zalecane działanie czyli próbować leczyć, a jeżeli nie jest to możliwe usuwać obiekt. Przed usunięciem zainfekowanego obiektu monitor antywirusowy powinien przenieść go w bezpieczny obszar dysku – kwarantanna, plik w kwarantannie powinien być zaszyfrowany.
* Rejestrować w pliku raportu informację o wykryciu wirusa
* Powiadamiać administratora przy użyciu poczty elektronicznej
1. Skaner antywirusowy może być uruchamiany automatycznie zgodnie z terminarzem; skanowane są wszystkie lokalne dyski twarde komputera.
2. System antywirusowy ma posiadać możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia.
3. Program powinien posiadać możliwość określenia harmonogramu pobierania uaktualnień, w tym możliwość wyłączenia aktualizacji automatycznej.
4. Program musi posiadać możliwość pobierania uaktualnień modułów dla zainstalowanej wersji aplikacji.
5. Program powinien posiadać możliwość określenia źródła uaktualnień.
6. Program musi posiadać możliwość określenia ustawień serwera proxy w przypadku, gdy jest on wymagany do nawiązania połączenia z Internetem.
7. Pobieranie uaktualnień w trybie przyrostowym (np. po zerwaniu połączenia, bez konieczności retransmitowania już wczytanych fragmentów informacji).
8. Program powinien posiadać możliwość określenia okresu przechowywania raportów.
9. Program powinien posiadać możliwość określenia okresu przechowywania obiektów znajdujących się w magazynie kopii zapasowych -kwarantannie.
10. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.

**III. Urządzenia Mobilne**

1. Możliwość pobrania wersji instalacyjnej ze sklepu Android

2. Skanowanie aplikacji w trakcie instalacji na urządzeniach z systemem Android

3. Posiadać możliwość wymuszenia szyfrowania urządzenia dla systemu Android

4. Możliwość blokowania ekranu głównego hasłem.

5. Kontrola przeglądarki.

# IV. Konsola

1. System scentralizowanego zarządzania powinien obsługiwać (umożliwiać zainstalowanie i działanie wszystkich modułów) następujące systemy operacyjne:

Windows Server 2022 Standard / Core / Datacenter 64-bitowy

Windows Server 2019 Standard / Core / Datacenter 64-bitowy

Windows Server 2016 Server Standard / Datacenter / Core 64-bitowy

Windows Server 2012 R2 Standard / Server Core / Essentials / Datacenter 64-bitowy

1. System scentralizowanego zarządzania powinien przechowywać ustawienia w bazie danych. Silnik bazy danych winien być dostarczony wraz z systemem lub też powinien być dostępny na darmowej licencji dla użytkowników biznesowych np. Microsoft SQL Server Express 64-bitowy
2. System zdalnego zarządzania powinien posiadać polskojęzyczny interfejs konsoli programu.
3. System zdalnego zarządzania winien zapewniać centralną instalację, konfigurację, aktualizację, zarządzanie oraz przeglądanie logów ochrony antywirusowej, antyspyware’owej, (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanej na stacjach roboczych i serwerach w sieci korporacyjnej z jednego serwera zarządzającego.
4. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w danej sieci w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.
5. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
6. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu
7. System zdalnego zarządzania powinien umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych.
8. Komunikacja pomiędzy serwerem zarządzającym a agentami sieciowymi na stacjach roboczych winna być szyfrowana przy użyciu protokołu SSL.
9. Konsola administracyjna ma posiadać możliwość zdalnego inicjowania skanowania antywirusowego na stacjach roboczych włączonych do sieci komputerowych w całej firmie.
10. Zarządzanie aplikacjami odbywa się przy użyciu profili aplikacji oraz zadań.
11. Konsola administracyjna ma możliwość informowania administratorów o wykryciu epidemii wirusa.
12. Serwer zarządzający ma mieć możliwość automatycznej reakcji na epidemie wirusa (automatyczne stosowanie wskazanego profilu ustawień stacji roboczych oraz uruchomienia odpowiednich zadań).
13. Możliwość tworzenia osobnych polityk ochrony dla fizycznych komputerów, serwerów, urządzeń mobilnych oraz maszyn wirtualnych
14. 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).
15. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.
16. System centralnego zarządzania wyposażony w mechanizmy raportowania i dystrybucji oprogramowania oraz polityk antywirusowych w sieciach korporacyjnych.
17. System centralnej dystrybucji i instalacji aktualizacji bibliotek sygnatur wirusów, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji biblioteki.
18. System centralnej dystrybucji i instalacji aktualizacji oprogramowania, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowego oprogramowania.
19. System centralnego zbierania informacji oraz ręcznego (na żądanie) i automatycznego (według harmonogramu) tworzenia sumarycznych raportów.
20. System zdalnego zarządzania powinien umożliwiać automatyczne wysyłanie raportów pocztą elektroniczną lub zapisywanie ich w postaci plików w zdefiniowanej lokalizacji (przynajmniej w formacie html).
21. System zdalnego zarządzania powinien umożliwiać podgląd w czasie rzeczywistym statystyk ochrony, stanu aktualizacji instalacji w sieci itp.
22. System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o aplikacjach znajdujących się na stacjach roboczych.
23. Program powinien mieć możliwość dezinstalacji aplikacji niekompatybilnych.
24. Program powinien dawać możliwość kontrolowania na stacjach roboczych aktualizacji systemowych oraz wymuszenia ich instalacji.
25. System zdalnego zarządzania powinien mieć możliwość zbierania informacji o sprzęcie zainstalowanym na komputerach klienckich.
26. System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o obiektach poddanych kwarantannie oraz podejmowanie odpowiednich działań (np. przywracanie, skanowanie, wysłanie do analizy itp.).
27. System zdalnego zarządzania powinien umożliwiać przeglądanie informacji o obiektach, które zostały wykryte ale program nie podjął względem nich żadnego działania wraz z możliwością wymuszenia przez administratora odpowiedniego działania.
28. System zdalnego zarządzania powinien umożliwiać automatyczne instalowanie licencji na stacjach roboczych.
29. System zdalnego zarządzania powinien umożliwiać automatyczne i regularne tworzenie kopii zapasowej serwera zarządzającego, która umożliwi przywrócenie w pełni działającego systemu zarządzania.
30. Program powinien umożliwić administratorowi wyłączenie niektórych lub wszystkich powiadomień wyświetlanych na stacjach roboczych.
31. System zdalnego zarządzania powinien mieć możliwość sprawdzenia aktualnych wersji oprogramowania antywirusowego.
32. System zdalnego zarządzania powinien umożliwiać zarządzanie poprawkami lub uaktualnieniami aplikacji firm trzecich.
33. System zdalnego zarządzania powinien umożliwić wysyłanie powiadomień do wybranych użytkowników przy użyciu min. poczty elektronicznej.
34. System zdalnego zarządzania powinien tworzyć repozytorium sprzętu min. komputerów i nośników wymiennych.
35. W całym okresie trwania subskrypcji użytkownik musi mieć prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
36. W całym okresie trwania subskrypcji użytkownik musi mieć możliwość pobierania i instalacji nowszych wersji oprogramowania i konsoli zarządzającej oraz aktualnych baz wirusowych.
37. System zdalnego zarządzania wraz z aplikacją na stacje robocze musi umożliwiać działanie w środowisku (sieci) izolowanym od internetu w dwóch scenariuszach:
	1. System całkowicie odizolowany od internetu. Aktualizacje aplikacji i baz wirusów przenoszone na nośniku wymiennym z komputera z dostępem do internetu na komputer z systemem zdalnego zarządzania w środowisku izolowanym. System winien zawierać aplikację przygotowującą repozytorium do przeniesienia.
	2. Tylko pojedyncze stacje w podsieciach majce dostęp do internetu w celu pobierania uaktualnień i udostępniające je stacjom z tej samej podsieci. Na stacjach tych nie może być zainstalowane oprogramowanie antywirusowe. System musi umożliwiać ograniczenie pasma sieciowego wykorzystywanego do pobierania uaktualnień.
38. System zdalnego zarządzania musi umożliwiać zarządzanie stacjami w różnych lokalizacjach/sieciach połączonych np. łączami VPN przy zapewnieniu przez Zamawiającego połączenia sieciowego z lokalizacji zdalnej do lokalizacji głównej.

Wraz z produktem wykonawca jest zobowiązany dostarczyć w języku polskim opis instalacji i konfiguracji systemu dla wymagań opisanych w pkt. 40