Załącznik nr 3 do SWZ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Dostawa oprogramowania w ramach projektu pn.: Cyberbezpieczny samorząd w Gminie Czersk**

**Zadanie jest dofinansowane w ramach Umowy o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0836/ FERC.02.02-CS.01-001/23/2024. Zadanie finansowane z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23.**

**Przedmiot zamówienia obejmuje:**

1. **Licencje UTM – 1 sztuka**

Przedłużenie licencji do posiadanego przez Zamawiającego urządzenia UTM Stormshield SN310 Premium UTM Security Pack  na 12 miesięcy.

1. **Oprogramowanie antywirusowe**

Oprogramowanie antywirusowe - okres ochrony: 2 lata, liczba stanowisk: 7

**Ochrona stacji roboczych - Windows**

1. Pełne wsparcie dla systemu Windows 10/Windows 11.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
4. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
5. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim oraz angielskim.

**Ochrona antywirusowa i antyspyware**

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
7. System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
9. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
13. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
14. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
15. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
16. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
17. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
18. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
19. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
20. Wbudowany konektor dla programów MS Outlook.
21. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
22. 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).
23. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
24. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
25. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
26. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
27. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
28. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
29. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
30. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
31. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
32. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
33. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
34. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
35. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
36. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
37. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
38. Możliwość automatycznego wysyłania nowych do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
39. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
40. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
41. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
42. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
43. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
44. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
45. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
46. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
47. Program ma umożliwiać 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.
48. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
49. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
50. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
51. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
52. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
53. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
54. 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 program 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 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,
* tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

1. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
2. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
3. Aplikacja musi posiadać dedykowaną funkcję, wykorzystującą technologię procesorów Intel (TDT) w zakresie zwiększenia skuteczności wykrywania zagrożeń wymuszających okup.
4. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
5. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
6. Program ma być wyposażony we 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.
7. Funkcja, generująca taki log, ma posiadać przynajmniej 3 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
8. Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
9. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
10. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
11. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
12. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
13. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
14. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
15. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
16. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
17. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli rodzicielskiej i kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
18. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
19. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
20. Możliwość podejrzenia informacji o licencji, która znajduje się w programie.
21. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
22. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
23. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
24. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
25. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.
26. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
27. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
28. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
29. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
30. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

**Ochrona przed spamem**

1. Ochrona antyspamowa dla programów pocztowych MS Outlook.
2. Program ma umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
3. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
4. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
5. Możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
6. Możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
7. Możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
8. Program ma domyślnie współpracować z folderem „Wiadomości-śmieci”, dostępnym w programie Microsoft Outlook.
9. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana”
10. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana”.
11. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

**Zapora osobista (personal firewall)**

1. Zapora osobista ma pracować w jednym z czterech trybów:

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

1. Program musi oceniać reguły zapory systemu Windows. 105. Możliwość tworzenia list sieci zaufanych.
2. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
3. 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.
4. Możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
5. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
6. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
7. Wykrywanie modyfikacji w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
8. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
9. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
10. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
11. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
12. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
13. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
14. Program musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów: z aplikacją lokalną, którą administrator wskazuje z listy, z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.

**Kontrola rodzicielska**

1. Aplikacja musi być wyposażona w zintegrowany moduł kontroli rodzicielskiej.
2. Moduł Kontroli rodzicielskiej musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane reguły filtrowania.
3. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
4. Dla kont użytkowników musi istnieć możliwość przypisania gotowych profili filtrowania kategorii.
5. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
6. Podstawowe kategorie, w jakie aplikacja musi być co najmniej wyposażona to: Osoby dorosłe, Agresywne, Alkohol i wyroby tytoniowe, Ukrywające tożsamość, Sztuka, Motoryzacja, Biznes i praca, Czaty i sieci społecznościowe, komunikacja, Działalność przestępcza, Oświata, Rodzina i wychowanie dzieci, Moda, Finanse, Żywność i napoje, Zdrowie, Hobby i zainteresowania, Dzieci, Styl życia, Aktualności, Zwierzęta domowe, Zagadnienia społeczne, polityczne i prawne, Nieruchomości, Religia, Nauka, Edukacja seksualna, Zakupy, Sport, Technologie, Podróże
7. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.
8. Dla poszczególnych kont użytkownik ma posiadać możliwość utworzenia wyjątków dla konkretnych adresów url, które mogą być wyświetlone nawet w przypadku, gdy dany adres znajduje się w którejkolwiek z blokowanych kategorii.
9. Aplikacja musi być wyposażona w moduł logowania zablokowanych stron oraz kategorii niezależnie od zalogowanego użytkownika.
10. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli rodzicielskiej.

**Ochrona Bankowości elektronicznej**

1. Aplikacja musi być wyposażona w moduł ochrony bankowości internetowej.
2. Przeglądarka powinna automatycznie szyfrować wszelkie dane wpisywane przez Użytkownika w formularzach internetowych. Szyfrowanie powinno odbywać się na poziomie odczytu znaków wpisywanych z klawiatury.
3. Użytkownik w każdym czasie musi mieć możliwość ręcznego uruchomienia przeglądarki w trybie zabezpieczonym modułem ochrony bankowości elektronicznej dla dowolnego adresu URL.
4. Praca w trybie bezpiecznym musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na pasku przeglądarki.

**Monitor sieci domowej**

1. Aplikacja ma posiadać moduł skanujący sieć domową, do której podłączony jest użytkownik, wyświetlając obecnie podłączone urządzenia sieciowe oraz sygnalizować nowo podłączane.
2. Wyświetlane hosty widoczne są pod ich nazwą NETBIOS, adresem IP oraz adresem MAC. Wraz z tymi informacjami wyświetlane muszą być informacje na temat ostatniego wykrycia hosta.
3. Wyświetlana nazwa hosta może być modyfikowana przez użytkownika.
4. Aplikacja musi być wyposażona w mechanizm umożliwiający tworzenie reguł dla ostatnio zablokowanej komunikacji, użytkownik musi mieć możliwość wyświetlania komunikacji, jaka była blokowana w ostatnim czasie (co najmniej ostanie 5,15,60 minut).
5. Użytkownik ma możliwość otwarcia interfejsu logowania się do swojego urządzenia brzegowego (routera itp.) poprzez link umieszczony w menu aplikacji.
6. Moduł ochrony sieci musi mieć możliwość przeprowadzenia audytu zabezpieczeń routera znajdującego się w sieci użytkownika.
7. System skanowania routera musi mieć możliwość wykrycia co najmniej otwartych portów sieciowych, zabezpieczenia konfiguracji urządzenia za pomocą domyślnych lub słabych haseł.
8. Moduł ochrony sieci domowej wykonujący skanowanie pod kątem otwartych portów powinien sprawdzać co najmniej porty 80, 443, 139, 445, 21, 22, 23.
9. Moduł musi wykrywać również urządzenia podłączone w sieci domowej należące do grupy produktów „Internet of Things”.
10. Moduł ten musi mieć możliwość wykrycia, czy urządzenie pracuje w sieci publicznej czy lokalnej. W przypadku sieci publicznej program musi wyświetlić ostrzeżenie użytkownikowi o ryzyku skanowania w takim trybie.

**Ochrona kamery internetowej**

1. Aplikacja ma umożliwiać kontrolę użycia kamery internetowej przez procesy znajdujące się w systemie jak i inne aplikacje.
2. W przypadku próby użycia kamery przez aplikację lub proces systemowy, użytkownikowi musi wyświetlić się stosowny komunikat ostrzegawczy.
3. Wykrycie próby użycia kamery musi dać użytkownikowi możliwość zezwolenia lub blokady takiej czynności.
4. Użytkownik może utworzyć listę aplikacji, które będą miały dostęp do kamery. Analogiczna lista musi zostać utworzona dla aplikacji, dla których wykonywana będzie blokada.

**Ochrona antykradzieżowa**

1. Program musi posiadać moduł umożliwiający powiązanie zainstalowanego w systemie pakietu ochrony z kontem utworzonym na dedykowanym serwisie online dostępnym za pomocą przeglądarki internetowej na serwerach producenta.
2. Po zalogowaniu do swojego indywidualnego konta na portalu producenta użytkownik powinien mieć wylistowane urządzenia, z którymi jest to konto powiązane.
3. Logowanie do portalu za pomocą przeglądarki internetowej musi odbywać się poprzez zabezpieczoną komunikację HTTPS.
4. Portal musi posiadać polski interfejs.
5. Użytkownik z poziomu swojego konta musi posiadać możliwość wykonania testu na widocznym w portalu swoim komputerze w celu weryfikacji poprawności działania modułu antykradzieżowego.
6. Wyzwolenie zadania testu musi wymagać potwierdzenia jego wykonania od strony użytkownika urządzenia, na którym test ma być wykonany.
7. W trakcie testu mechanizmy wbudowane w pakiet antywirusowy muszą zebrać co najmniej informację o: lokalizacji testowanego komputera ( jeśli jest ona dostępna ) – urządzenie powinno być wskazane na mapie w postaci graficznej, wykonać screenshoot’a pulpitu oraz wykonać zdjęcie za pomocą wbudowanej w komputer kamery (jeśli jest dostępna) i zebrać informację o adresie IP, z jakiego łączy się testowany komputer.
8. Zebrane podczas testów informacje muszą być widoczne dla zalogowanego na portalu użytkownika.
9. W przypadku kradzieży lub zagubienia urządzenia, Użytkownik musi posiadać możliwość określenia swojego urządzenia jako brakującego.
10. W momencie, gdy urządzenie zostanie określone jako brakujące, automatycznie musi zostać przesłane na nie zadanie aktywacji dedykowanego konta systemowego z ograniczeniami, oraz wymuszenie restartu systemu Windows.
11. Po restarcie komputera musi istnieć możliwość zalogowania się jedynie do konta z ograniczeniami utworzonego przez mechanizmy auto ochrony, pozostałe konta systemowe mają być nieaktywne.
12. Mechanizm antykradzieżowy w momencie aktywacji ma automatycznie tworzyć zdjęcia przy wykorzystaniu wbudowanej w urządzenie kamery (jeśli dostępna), zapisywać obraz pulpitu, zbierać informacje odnośnie lokalizacji urządzenia oraz wykorzystywanych adresów IP.
13. Zebrane informacje mają zostać przesłane na konto użytkownika utworzone na portalu producenta.
14. W przypadku braku połączenia z siecią Internet, w/w informacje maja być zbierane i przesłane do portalu w momencie, gdy urządzenie będzie posiadało aktywne połączenie z siecią Internet.
15. Zalogowany do konta na portalu producenta użytkownik musi posiadać możliwość zdalnego wyświetlenia na brakującym urządzeniu dowolnego komunikatu zawierającego tekst i obraz.
16. Z poziomu portalu, użytkownik musi mieć dostęp do danych historycznych wcześniej zebranych podczas testów lub w momencie określenia urządzenia jako brakującego.
17. Użytkownik musi posiadać opcję usunięcia swojego konta z serwerów producenta wraz z informacjami tam się znajdującymi.

**Menedżer licencji**

1. Interfejs menedżera licencji musi być dostępny z poziomu strony WWW.
2. Dostęp do witryny musi być zabezpieczony z pomocą SSL.
3. Interfejs webowy musi być dostępny w języku polskim.
4. Interfejs www musi posiadać możliwość dodania więcej niż jednej licencji.
5. Produkt zabezpieczający musi posiadać możliwość aktywacji przy pomocy danych logowania menedżera licencji.
6. Komputer po aktywacji musi się zgłaszać do menedżera licencji za pomocą nazwy NETBIOS.
7. Menedżer musi pokazywać liczbę wykorzystanych i dostępnych licencji.
8. Musi być możliwość zmiany nazwy komputera na stornie www po dokonaniu aktywacji .
9. Dezaktywacja licencji musi być dostępna bezpośrednio z interfejsu www.
10. Przy usuwaniu licencji z interfejsu www musi być dostępna opcja dezaktywacji wszystkich stacji.

**Prywatność i zabezpieczenia przeglądarki**

1. Czyszczenie danych przeglądarki musi być obsługiwane przez rozszerzenie instalowane bezpośrednio w przeglądarkach Google Chrome, Mozilla Firefox oraz Microsoft Edge.
2. Produkt musi pozwalać na usuwanie danych przeglądarki, minimum: historia pobierania, historia przeglądania, pliki cookie, obrazy i pliki zapisane w pamięci podręcznej, hasła i dane logowania, autouzupełnianie danych formularzy.
3. Produkt musi zezwalać na tworzenie listy stron internetowych, których czyszczenie danych przeglądarki nie dotyczy.
4. Produkt musi pozwalać na czyszczenie w trybie jednorazowym bądź cyklicznym.
5. Produkt musi posiadać funkcjonalność skanującą wyniki wyszukiwania i wyświetlać informacje o tym czy witryna jest bezpieczna.

**Sandbox w chmurze**

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. 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.
4. Użytkownik musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Użytkownik musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Użytkownik musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
8. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej.

W przypadku wykrycia zagrożenia, komputer jest bezzwłocznie chroniony.

1. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

**Menadżer haseł**

1. Produkt musi posiadać narzędzie do przechowywania oraz zabezpieczania haseł i danych osobowych zdefiniowanych przez użytkownika.
2. Narzędzie to musi być dostępne na systemach Windows, macOS, Andorid oraz iOS.
3. Narzędzie to musi integrować się z przeglądarkami Microsoft Edge, Mozilla Firefox, Google Chrome.
4. Narzędzie musi posiadać funkcjonalność generowania nowych haseł, posiadających do 32 znaków.
5. Narzędzie musi posiadać funkcjonalność raportowania, która poinformuje m. in. o tym czy hasła jest słabe.
6. Narzędzie musi posiadać funkcjonalność zdalnego wylogowania z kont.

**Szyfrowanie danych**

1. Produkt musi posiadać funkcjonalność szyfrowania danych znajdujących się na dyskach wewnętrznych oraz wymiennych
2. Szyfrowanie danych musi odbywać się z wykorzystaniem algorytmu AES 256.
3. Zaszyfrowane dane na nośnikach wymiennych muszą być zdatne do odczytu na urządzeniu bez konieczności posiadania produktu zabezpieczającego.
4. **Oprogramowanie antywirusowe**

Oprogramowanie antywirusowe - okres ochrony: 2 lata, minimum 8 stanowisk.

**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**

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 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).
11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
12. 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.
13. 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.
14. 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.
15. 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.

1. 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.
2. 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.
3. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
4. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
5. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

**Ochrona serwera**

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 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:

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. 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.
6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.*
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
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.

**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.

1. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
2. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
3. nazwę aplikacji,
4. nazwę pakietu,
5. kategorię sklepu Google Play,
6. uprawnienia aplikacji,
7. pochodzenie aplikacji z nieznanego źródła.

1. **Oprogramowanie antywirusowe – 2 sztuki**

Oprogramowanie antywirusowe - okres ochrony: 2 lata, minimum 5 stanowisk.

**Ochrona stacji roboczych - Windows**

1. Pełne wsparcie dla systemu Windows 10/Windows 11.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
4. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
5. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim oraz angielskim.

**Ochrona antywirusowa i antyspyware**

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
7. System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
9. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
13. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
14. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
15. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
16. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
17. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
18. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
19. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
20. Wbudowany konektor dla programów MS Outlook.
21. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
22. 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).
23. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
24. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
25. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
26. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
27. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
28. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
29. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
30. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
31. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
32. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
33. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
34. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
35. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
36. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
37. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
38. Możliwość automatycznego wysyłania nowych do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
39. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
40. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
41. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
42. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
43. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
44. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
45. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
46. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
47. Program ma umożliwiać 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.
48. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
49. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
50. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
51. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
52. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
53. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
54. 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 program 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 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,
* tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

1. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
2. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
3. Aplikacja musi posiadać dedykowaną funkcję, wykorzystującą technologię procesorów Intel (TDT) w zakresie zwiększenia skuteczności wykrywania zagrożeń wymuszających okup.
4. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
5. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
6. Program ma być wyposażony we 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.
7. Funkcja, generująca taki log, ma posiadać przynajmniej 3 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
8. Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
9. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
10. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
11. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
12. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
13. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
14. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
15. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
16. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
17. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli rodzicielskiej i kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
18. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
19. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
20. Możliwość podejrzenia informacji o licencji, która znajduje się w programie.
21. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
22. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
23. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
24. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
25. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.
26. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
27. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
28. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.*
29. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
30. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

**Ochrona przed spamem**

1. Ochrona antyspamowa dla programów pocztowych MS Outlook.
2. Program ma umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
3. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
4. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
5. Możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
6. Możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
7. Możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
8. Program ma domyślnie współpracować z folderem „Wiadomości-śmieci”, dostępnym w programie Microsoft Outlook.
9. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana”
10. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana”.
11. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

**Zapora osobista (personal firewall)**

1. Zapora osobista ma pracować w jednym z czterech trybów:

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

1. Program musi oceniać reguły zapory systemu Windows. 105. Możliwość tworzenia list sieci zaufanych.
2. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
3. 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.
4. Możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
5. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
6. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
7. Wykrywanie modyfikacji w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
8. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
9. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
10. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
11. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
12. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
13. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
14. Program musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów: z aplikacją lokalną, którą administrator wskazuje z listy, z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.

**Kontrola rodzicielska**

1. Aplikacja musi być wyposażona w zintegrowany moduł kontroli rodzicielskiej.
2. Moduł Kontroli rodzicielskiej musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane reguły filtrowania.
3. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
4. Dla kont użytkowników musi istnieć możliwość przypisania gotowych profili filtrowania kategorii.
5. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
6. Podstawowe kategorie, w jakie aplikacja musi być co najmniej wyposażona to: Osoby dorosłe, Agresywne, Alkohol i wyroby tytoniowe, Ukrywające tożsamość, Sztuka, Motoryzacja, Biznes i praca, Czaty i sieci społecznościowe, komunikacja, Działalność przestępcza, Oświata, Rodzina i wychowanie dzieci, Moda, Finanse, Żywność i napoje, Zdrowie, Hobby i zainteresowania, Dzieci, Styl życia, Aktualności, Zwierzęta domowe, Zagadnienia społeczne, polityczne i prawne, Nieruchomości, Religia, Nauka, Edukacja seksualna, Zakupy, Sport, Technologie, Podróże
7. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.
8. Dla poszczególnych kont użytkownik ma posiadać możliwość utworzenia wyjątków dla konkretnych adresów url, które mogą być wyświetlone nawet w przypadku, gdy dany adres znajduje się w którejkolwiek z blokowanych kategorii.
9. Aplikacja musi być wyposażona w moduł logowania zablokowanych stron oraz kategorii niezależnie od zalogowanego użytkownika.
10. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli rodzicielskiej.

**Ochrona Bankowości elektronicznej**

1. Aplikacja musi być wyposażona w moduł ochrony bankowości internetowej.
2. Przeglądarka powinna automatycznie szyfrować wszelkie dane wpisywane przez Użytkownika w formularzach internetowych. Szyfrowanie powinno odbywać się na poziomie odczytu znaków wpisywanych z klawiatury.
3. Użytkownik w każdym czasie musi mieć możliwość ręcznego uruchomienia przeglądarki w trybie zabezpieczonym modułem ochrony bankowości elektronicznej dla dowolnego adresu URL.
4. Praca w trybie bezpiecznym musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na pasku przeglądarki.

**Monitor sieci domowej**

1. Aplikacja ma posiadać moduł skanujący sieć domową, do której podłączony jest użytkownik, wyświetlając obecnie podłączone urządzenia sieciowe oraz sygnalizować nowo podłączane.
2. Wyświetlane hosty widoczne są pod ich nazwą NETBIOS, adresem IP oraz adresem MAC. Wraz z tymi informacjami wyświetlane muszą być informacje na temat ostatniego wykrycia hosta.
3. Wyświetlana nazwa hosta może być modyfikowana przez użytkownika.
4. Aplikacja musi być wyposażona w mechanizm umożliwiający tworzenie reguł dla ostatnio zablokowanej komunikacji, użytkownik musi mieć możliwość wyświetlania komunikacji, jaka była blokowana w ostatnim czasie (co najmniej ostanie 5,15,60 minut).
5. Użytkownik ma możliwość otwarcia interfejsu logowania się do swojego urządzenia brzegowego (routera itp.) poprzez link umieszczony w menu aplikacji.
6. Moduł ochrony sieci musi mieć możliwość przeprowadzenia audytu zabezpieczeń routera znajdującego się w sieci użytkownika.
7. System skanowania routera musi mieć możliwość wykrycia co najmniej otwartych portów sieciowych, zabezpieczenia konfiguracji urządzenia za pomocą domyślnych lub słabych haseł.
8. Moduł ochrony sieci domowej wykonujący skanowanie pod kątem otwartych portów powinien sprawdzać co najmniej porty 80, 443, 139, 445, 21, 22, 23.
9. Moduł musi wykrywać również urządzenia podłączone w sieci domowej należące do grupy produktów „Internet of Things”.
10. Moduł ten musi mieć możliwość wykrycia, czy urządzenie pracuje w sieci publicznej czy lokalnej. W przypadku sieci publicznej program musi wyświetlić ostrzeżenie użytkownikowi o ryzyku skanowania w takim trybie.

**Ochrona kamery internetowej**

1. Aplikacja ma umożliwiać kontrolę użycia kamery internetowej przez procesy znajdujące się w systemie jak i inne aplikacje.
2. W przypadku próby użycia kamery przez aplikację lub proces systemowy, użytkownikowi musi wyświetlić się stosowny komunikat ostrzegawczy.
3. Wykrycie próby użycia kamery musi dać użytkownikowi możliwość zezwolenia lub blokady takiej czynności.
4. Użytkownik może utworzyć listę aplikacji, które będą miały dostęp do kamery. Analogiczna lista musi zostać utworzona dla aplikacji, dla których wykonywana będzie blokada.

**Ochrona antykradzieżowa**

1. Program musi posiadać moduł umożliwiający powiązanie zainstalowanego w systemie pakietu ochrony z kontem utworzonym na dedykowanym serwisie online dostępnym za pomocą przeglądarki internetowej na serwerach producenta.
2. Po zalogowaniu do swojego indywidualnego konta na portalu producenta użytkownik powinien mieć wylistowane urządzenia, z którymi jest to konto powiązane.
3. Logowanie do portalu za pomocą przeglądarki internetowej musi odbywać się poprzez zabezpieczoną komunikację HTTPS.
4. Portal musi posiadać polski interfejs.
5. Użytkownik z poziomu swojego konta musi posiadać możliwość wykonania testu na widocznym w portalu swoim komputerze w celu weryfikacji poprawności działania modułu antykradzieżowego.
6. Wyzwolenie zadania testu musi wymagać potwierdzenia jego wykonania od strony użytkownika urządzenia, na którym test ma być wykonany.
7. W trakcie testu mechanizmy wbudowane w pakiet antywirusowy muszą zebrać co najmniej informację o: lokalizacji testowanego komputera ( jeśli jest ona dostępna ) – urządzenie powinno być wskazane na mapie w postaci graficznej, wykonać screenshoot’a pulpitu oraz wykonać zdjęcie za pomocą wbudowanej w komputer kamery (jeśli jest dostępna) i zebrać informację o adresie IP, z jakiego łączy się testowany komputer.
8. Zebrane podczas testów informacje muszą być widoczne dla zalogowanego na portalu użytkownika.
9. W przypadku kradzieży lub zagubienia urządzenia, Użytkownik musi posiadać możliwość określenia swojego urządzenia jako brakującego.
10. W momencie, gdy urządzenie zostanie określone jako brakujące, automatycznie musi zostać przesłane na nie zadanie aktywacji dedykowanego konta systemowego z ograniczeniami, oraz wymuszenie restartu systemu Windows.
11. Po restarcie komputera musi istnieć możliwość zalogowania się jedynie do konta z ograniczeniami utworzonego przez mechanizmy auto ochrony, pozostałe konta systemowe mają być nieaktywne.
12. Mechanizm antykradzieżowy w momencie aktywacji ma automatycznie tworzyć zdjęcia przy wykorzystaniu wbudowanej w urządzenie kamery (jeśli dostępna), zapisywać obraz pulpitu, zbierać informacje odnośnie lokalizacji urządzenia oraz wykorzystywanych adresów IP.
13. Zebrane informacje mają zostać przesłane na konto użytkownika utworzone na portalu producenta.
14. W przypadku braku połączenia z siecią Internet, w/w informacje maja być zbierane i przesłane do portalu w momencie, gdy urządzenie będzie posiadało aktywne połączenie z siecią Internet.
15. Zalogowany do konta na portalu producenta użytkownik musi posiadać możliwość zdalnego wyświetlenia na brakującym urządzeniu dowolnego komunikatu zawierającego tekst i obraz.
16. Z poziomu portalu, użytkownik musi mieć dostęp do danych historycznych wcześniej zebranych podczas testów lub w momencie określenia urządzenia jako brakującego.
17. Użytkownik musi posiadać opcję usunięcia swojego konta z serwerów producenta wraz z informacjami tam się znajdującymi.

**Menedżer licencji**

1. Interfejs menedżera licencji musi być dostępny z poziomu strony WWW.
2. Dostęp do witryny musi być zabezpieczony z pomocą SSL.
3. Interfejs webowy musi być dostępny w języku polskim.
4. Interfejs www musi posiadać możliwość dodania więcej niż jednej licencji.
5. Produkt zabezpieczający musi posiadać możliwość aktywacji przy pomocy danych logowania menedżera licencji.
6. Komputer po aktywacji musi się zgłaszać do menedżera licencji za pomocą nazwy NETBIOS.
7. Menedżer musi pokazywać liczbę wykorzystanych i dostępnych licencji.
8. Musi być możliwość zmiany nazwy komputera na stornie www po dokonaniu aktywacji .
9. Dezaktywacja licencji musi być dostępna bezpośrednio z interfejsu www.
10. Przy usuwaniu licencji z interfejsu www musi być dostępna opcja dezaktywacji wszystkich stacji.

**Prywatność i zabezpieczenia przeglądarki**

1. Czyszczenie danych przeglądarki musi być obsługiwane przez rozszerzenie instalowane bezpośrednio w przeglądarkach Google Chrome, Mozilla Firefox oraz Microsoft Edge.
2. Produkt musi pozwalać na usuwanie danych przeglądarki, minimum: historia pobierania, historia przeglądania, pliki cookie, obrazy i pliki zapisane w pamięci podręcznej, hasła i dane logowania, autouzupełnianie danych formularzy.
3. Produkt musi zezwalać na tworzenie listy stron internetowych, których czyszczenie danych przeglądarki nie dotyczy.
4. Produkt musi pozwalać na czyszczenie w trybie jednorazowym bądź cyklicznym.
5. Produkt musi posiadać funkcjonalność skanującą wyniki wyszukiwania i wyświetlać informacje o tym czy witryna jest bezpieczna.

**Sandbox w chmurze**

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. 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.
4. Użytkownik musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Użytkownik musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Użytkownik musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
8. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej.

W przypadku wykrycia zagrożenia, komputer jest bezzwłocznie chroniony.

1. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

**Menadżer haseł**

1. Produkt musi posiadać narzędzie do przechowywania oraz zabezpieczania haseł i danych osobowych zdefiniowanych przez użytkownika.
2. Narzędzie to musi być dostępne na systemach Windows, macOS, Andorid oraz iOS.
3. Narzędzie to musi integrować się z przeglądarkami Microsoft Edge, Mozilla Firefox, Google Chrome.
4. Narzędzie musi posiadać funkcjonalność generowania nowych haseł, posiadających do 32 znaków.
5. Narzędzie musi posiadać funkcjonalność raportowania, która poinformuje m. in. o tym czy hasła jest słabe.
6. Narzędzie musi posiadać funkcjonalność zdalnego wylogowania z kont.

**Szyfrowanie danych**

1. Produkt musi posiadać funkcjonalność szyfrowania danych znajdujących się na dyskach wewnętrznych oraz wymiennych
2. Szyfrowanie danych musi odbywać się z wykorzystaniem algorytmu AES 256.
3. Zaszyfrowane dane na nośnikach wymiennych muszą być zdatne do odczytu na urządzeniu bez konieczności posiadania produktu zabezpieczającego.
4. **Oprogramowanie przeciwdziałające wyciekowi danych – 77 sztuk**

Licencja wieczysta z 2 letnim okresem wsparcia dla 77 stanowisk.

Oprogramowanie przeciwdziałające wyciekowi danych w łącznej ilości 77 sztuk rozdzielonej na osobne paczki zarządzane oddzielnie w ilościach:

* 7 sztuk,
* 15 sztuk,
* 55 sztuk,

Minimalne wymagania Zamawiającego

**Ochrona przed wyciekiem danych**

1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows 11 z najnowszymi aktualizacjami.
2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych.
3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim.
4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL.
6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
8. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.
9. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.
11. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania: kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.
12. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.
13. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania.
14. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.
15. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:

* Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
* Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.

1. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory.
2. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:
3. logowanie oraz wylogowanie użytkownika,
4. włączenie oraz wyłączenie stacji roboczej,
5. blokada oraz odblokowanie stacji roboczej,
6. przejście w stan bezczynności stacji roboczej.
7. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie zbliżonym do rzeczywistego.
8. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.
9. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.
10. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF bądź XLS.
11. Serwer musi posiadać możliwość wysłania alertów co najmniej za pośrednictwem wiadomości email oraz za pomocą SIEM/SYSLOG.
12. Serwer administracyjny musi posiadać możliwość konfiguracji cyklicznych raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
13. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
14. Raporty muszą być generowane do pliku PDF i/lub XLS, zapisywane w lokalizacji na serwerze lub na wskazany adres(y) e-mail.
15. Serwer administracyjny musi posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania, ale również umożliwiać jego zmianę na serwer klienta.
16. Serwer administracyjny musi posiadać możliwość wyszukiwania plików w oparciu o ich zawartość, co najmniej o:

a) numery kart kredytowych,

b) numer PESEL,

c) numer polskiego dowodu osobistego,

d) polski numer paszportu,

e) wyrażenia regularne,

f) określone ciągi znaków,

g) numer IBAN.

1. Weryfikacja zawartości pliku powinna odbywać się w czasie rzeczywistym.
2. System musi posiadać możliwość importu własnych słowników do klasyfikowania danych.
3. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych od jakich plik zostanie sklasyfikowany.
4. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na:

a) audyt i logowanie wiadomości e-mail,

b) audyt i logowanie operacji na plikach.

1. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi.
2. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:

a) Bezpieczeństwo danych:

• Przegląd informacji o incydentach bezpieczeństwa.

• Przegląd danych przychodzących.

• Przegląd danych wychodzących.

• Przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików.

• Podłączane/odłączane urządzenia przenośne.

b) Produktywność:

• Przegląd informacji na temat produktywności użytkowników.

• Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.

c) Eksploatacja sprzętu:

• Przegląd informacji na temat eksploatacji sprzętu komputerowego.

• Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.

• Eksploatacja drukarek.

• Eksploatacji sieci.

1. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.
2. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
3. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt:

• plików przenoszonych na nośniki USB i inne urządzenia przenośne,

• plików przesłanych za pomocą wiadomości e-mail,

• plików przesłanych za pomocą poczty webowej,

• plików przesłanych do Internetu,

• plików wysłanych za pomocą komunikatorów,

• plików przesłanych na dyski chmurowe,

• analiza sposobu korzystania z aplikacji,

• analiza korzystania z Internetu,

• analiza wykorzystania portali do poszukiwania pracy

1. **Wdrożenie systemów teleinformatycznych**

Usługi wdrożeniowe oprogramowania przeciwdziałającego wyciekowi danych (DLP), którego głównym celem jest zabezpieczenie przed utratą lub nieautoryzowanym dostępem do informacji poufnych. Oprogramowanie to ma zostać zainstalowane na serwerze działającym pod kontrolą systemu Windows Server co najmniej w wersji 2016 oraz powinno być obsługiwane za pomocą dwóch konsol: aplikacyjnej i webowej, w celu ułatwienia zarządzania systemem.

1. Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.
2. Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.
3. Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.
4. Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.
5. Wykonawca zainstaluje oprogramowanie przeciwdziałającego wyciekowi danych.
6. Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.
7. Wykonawca uruchomieni i skonfiguruje konsolę zarządzającą, wprowadzi klucz dostępowy i usunie dane demonstracyjne.
8. Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.
9. Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze oraz urządzeniach końcowych.
10. Wykonawca wykona konfigurację kategorii danych i danych wrażliwych oraz zdefiniuje wykrywanie kategorii:

* Numery kart kredytowych
* Numery IBAN
* Numery dowodów osobistych
* Polski numer paszportu
* Numer PESEL

1. Wykonawca skonfiguruje alerty związane z usługami oraz zabezpieczeniem DLP oraz przetestuje poprawność ich działania na danych testowych.
2. Wykonawca skonfiguruje zadania archiwizacji danych oraz usuwania starych wpisów z bazy danych.
3. Wykonawca przetestuje działanie polityk i wprowadzi ich aktualizację w przypadku wykrycia braku ich skutecznego działania.
4. Wykonawca wygeneruje z prawidłowo wdrożonego oprogramowania raport audytu bezpieczeństwa i przeprowadzi analizę aktywności użytkowników oraz przepływu informacji w organizacji.
5. Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje.
6. Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.
7. Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii.

W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych Wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia   
w wystarczająco precyzyjny i zrozumiały sposób i jest to uzasadnione specyfiką przedmiotu zamówienia.   
W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”. W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, ocen technicznych, specyfikacji technicznych   
i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 Pzp, **Zamawiający dopuszcza rozwiązania równoważne opisywanym,** **a wskazane powyżej odniesienia należy odczytywać   
z wyrazami „lub równoważne”.** Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i funkcjonalne spełniające co najmniej warunki określone w opisie przedmiotu zamówienia. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany udowodnić w ofercie, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w szczegółowym opisie przedmiotu zamówienia.