Specyfikacja wymagań

Spis treści

PLATFORMA OCHRONY AUTOMATYCZNEJ

Części składowe:

- I.a. Oprogramowanie ochrony automatycznej,
- I.b. Oprogramowanie zapewniające automatyczną ochronę rozbudowanych sieci,
- I.c. Licencja na oprogramowanie ochrony serwera pocztowego.

Ad. I.a. Oprogramowanie ochrony automatycznej

- **Wymagania Ogólne**

Dostarczone oprogramowanie bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa. Dopuszcza się aby poszczególne elementy wchodzące w skład oprogramowania bezpieczeństwa były zrealizowane w postaci osobnych aplikacji instalowanych na platformach ogólnego przeznaczenia.

Oprogramowanie realizujące funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego oprogramowania bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

Oprogramowanie musi wspierać IPv4 oraz IPv6 w zakresie firewall, ochrony w warstwie aplikacji, protokołów routingu dynamicznego.

- **Redundancja, monitoring i wykrywanie awarii:**

1. W przypadku oprogramowania pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. Oprogramowanie musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

- **Interfejsy:**

W ramach oprogramowania Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 7.4 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps.
4. Wydajność szyfrowania IPSec VPN: nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 500 Mbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 130 Mbps.

- **Funkcje Oprogramowania Bezpieczeństwa:**

W ramach dostarczonego oprogramowania ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych platform lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

- **Polityki, Firewall:**

1. Oprogramowanie Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW.
1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. Oprogramowanie musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: Translację jeden do jeden oraz jeden do wielu, Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach oprogramowania musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

- **Połączenia VPN**

1. Oprogramowanie musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
    a. Wsparcie dla IKE v1 oraz v2.
    b. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
    c. Obsługa protokołu Diffie-Hellman grup 19 i 20.
    d. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
    e. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
    f. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
    g. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
    h. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
    i. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. Oprogramowanie musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
    a. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
    b. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

- **Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: Routingu statycznego .
    - Policy Based Routingu.
    - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
2. Oprogramowanie musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

- **Zarządzanie pasmem**
    1. Oprogramowanie Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
    2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
    3. Oprogramowanie musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
- **Kontrola Antywirusowa**
    1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
    2. Oprogramowanie musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
    3. Oprogramowanie musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
    4. Oprogramowanie musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
- **Ochrona przed atakami**
    1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
    2. Oprogramowanie powinnno chronić przed atakami na aplikacje pracujące na niestandardowych portach.
    3. Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
    4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
    5. Oprogramowanie musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
    6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
    7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
- **Kontrola aplikacji**
    1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
    2. Baza Kontroli Aplikacji powinna zawierać minimum 2500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
    3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
    4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

- **Kontrola WWW**
  1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
  2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
  3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
  4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
  5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
- **Uwierzytelnianie użytkowników w ramach sesji**
  1. Oprogramowanie Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
     a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
     b. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
     c. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
  2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
  3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
- **Zarządzanie**
  1. Elementy oprogramowania bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
  2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
  3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
  4. Oprogramowanie musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
  5. Oprogramowanie musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
  6. Element oprogramowania pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
- **Logowanie**
  1. Elementy oprogramowania bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
  2. W ramach logowania oprogramowanie pełniące funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności

administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

- **Certyfikaty**

Poszczególne elementy oferowanego oprogramowania bezpieczeństwa powinny posiadać następujące certyfikacje:

a. ICSA lub EAL4 dla funkcji Firewall,
b. ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW,
c. ICSA dla funkcji SSL VPN.

- **Serwisy i licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów co najmniej do dnia 31/03/2023. Powinny one obejmować kontrolę aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), analiza typu Sandbox, antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

- **Gwarancja oraz wsparcie**

Oprogramowanie musi być objęty serwisem gwarancyjnym producenta przez okres co najmniej do 31/03/2023. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

Ad. I.b. Oprogramowanie zapewniające automatyczną ochronę rozbudowanych sieci

Wymagania:

- **Licencje i aktualizacje**

Oprogramowanie powinno posiadać możliwość aktualizacji i aktualizacji baz sygnatur do najmniej do 31/03/2023. Oprogramowanie powinno posiadać licencje do zabezpieczenia co najmniej 150 punktów tj. stacji roboczych, serwerów, urządzeń mobilnych

- **Ochrona stacji roboczych - Windows**

1. Pełne wsparcie dla systemu Windows 7/Windows 10.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dostępna 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.
6. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives.

- **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. Oprogramowanie 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).
9. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
12. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
13. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
14. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
15. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.

16. 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.
17. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
18. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
19. 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).
20. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
21. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
22. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
23. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
24. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
25. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
26. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
27. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
28. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
29. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
30. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
31. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
32. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
33. 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.
34. 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.
35. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy

użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.

36. 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.
37. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
38. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
39. 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.
40. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
41. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
42. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
43. 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.
44. 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.
45. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
46. 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.
47. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
48. W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
49. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
50. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
51. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje,
    b. reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    a. tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

b. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
c. 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,
d. tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

52. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
53. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
54. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
55. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
56. 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.
57. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
58. 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.
59. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
60. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
61. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
62. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
63. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają vwszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
64. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
65. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
66. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
67. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron internetowych i kontroli dostępu do urządzeń, skanowania oraz zdarzeń.

68. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
69. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
70. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
71. Możliwość podejrzenia informacji o licencji, która znajduje się w programie.
72. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM.
73. W programie musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
74. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.
75. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
76. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
77. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
78. Program musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
79. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
80. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
81. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
82. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
83. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
84. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
85. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
86. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.
87. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
88. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.

89. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
90. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.
91. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
92. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
93. 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, Outlook Express, Windows Mail oraz Windows Live Mail.
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**

1. Zapora osobista ma pracować w jednym z czterech trybów:
   a. tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
   b. tryb interaktywny – program pyta się o każde nowo nawiązywane połączenie,
   c. tryb oparty na regułach – program blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
   d. tryb uczenia się – program automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

2. Program musi oceniać reguły zapory systemu Windows.
3. Możliwość tworzenia list sieci zaufanych.
4. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
5. 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.
6. Możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
7. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
8. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
9. Wykrywanie modyfikacji w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
10. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
11. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
12. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
13. 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.
14. 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.
15. 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.
16. Program musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem.
17. Musi pozwalać na rozwiązanie problemów:
    a. z aplikacją lokalną, którą administrator wskazuje z listy,
    b. z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.

- **Kontrola dostępu do stron internetowych**
    1. Aplikacja musi być wyposażona w zintegrowany moduł kontroli dostępu do stron internetowych.
    2. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
    3. Aplikacja musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
    4. Podstawowe kategorie, w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie,

zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.

5. Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych.
6. Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta.
7. Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do
8. stron internetowych.
9. Aplikacja musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj.
10. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.

- **Bezpieczna przeglądarka**
  1. Aplikacja musi być wyposażona w moduł bezpiecznej przeglądarki.
  2. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
  3. Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn,
  4. musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki.
  5. Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę.
  6. Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki.
  7. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

- **Stacje Robocze Apple Mac OS X**
  1. Pełne wsparcie dla systemów Mac OS X 10.12 lub nowszych.
  2. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
  3. Pomoc w programie (help) w języku polskim oraz angielskim.
  4. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
  5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing,
  6. narzędzi hakerskich, backdoor, itp.
  7. W momencie wykrycia trybu pełnoekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.
  8. Skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
  9. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
  10. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności).
  11. Możliwość skanowania dysków sieciowych i dysków przenośnych.
  12. Skanowanie plików spakowanych i skompresowanych.
  13. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów

lub plików o określonych rozszerzeniach.

14. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
15. 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.
16. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
17. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
18. Możliwość wykonania skanowania i wysłania pliku do analizy z poziomu menu kontekstowego.
19. Aktualizacje modułów analizy heurystycznej.
20. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie mają być wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
21. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e- mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
22. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
23. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
24. Ochrona przed atakami typu „phishing”.
25. Funkcja blokowania nośników wymiennych ma umożliwiać wyłączenie dostępu do nośników: Płyta CD/DVD, Pamięć masowa, karty sieciowe, Drukarka USB, Urządzenie do tworzenia obrazów, Port szeregowy, Urządzenie przenośne.
26. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
27. Aktualizacja modułów programu antywirusowego ma być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy serwera HTTP.
28. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
29. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po wystąpieniu zdarzenia).
30. Program umożliwia automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego.
31. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
32. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania oraz dokonanym skanowaniem komputera.
33. Program ma umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień.
34. Program musi posiadać mechanizm Ochrony dostępu do stron internetowych monitoruje komunikację w ramach protokołu HTTP.

35. Program musi pozwalać na konfigurację portów, dla których ma się odbywać skanowanie protokołu HTTP.
36. Program ma umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy” na modyfikację konfiguracji programu.
37. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
38. Możliwość zdalnego zarządzania programem z poziomu Administracji zdalnej.
39. Ochrona poczty mail:
    a. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej niezależnie od programu pocztowego.
    b. 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).
    c. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
    d. Możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
    e. Możliwość opcjonalnego dołączenia informacji w temacie zainfekowanej wiadomości o jej przeskanowaniu.
    f. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
40. Zapora osobista:
    a. Zapora osobista może pracować jednym z 2 trybów:
        - Automatyczny z wyjątkami - umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł,
        - Interaktywny – dla każdej nieznanej komunikacji generowane jest pytanie dla użytkownika o jej odblokowanie.
    b. Możliwość dezaktywacji funkcji zapory sieciowej.
    c. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
    d. Możliwość odnotowania faktu nawiązania danego połączenia w dzienniku zdarzeń.
    e. Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.
    f. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla profilu: Publiczny, Praca, Dom.
    g. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu
    h. IPv6.
    i. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
    j. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
    k. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
    l. Aktywacja stref ma się odbywać min. w oparciu o: interfejs sieciowy w systemie, Sieć WiFi, Podsieć IPv4/IPv6, Zakres adresów IPv4/IPv6, Adres IPv4/IPv6.
41. Kontrola dostępu do stron internetowych:
    a. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.

b. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
c. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
d. Reguły mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
e. Aplikacja musi posiadać możliwość filtrowania URL w oparciu o co najmniej 140 kategorii i podkategorii.
f. Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
g. Lista adresów URL, znajdujących się w poszczególnych kategoriach, musi być na bieżąco aktualizowana przez producenta.
h. Użytkownik musi posiadać możliwość wyłączenia modułu kontroli dostępu do stron internetowych.

- **Stacje robocze Linux**

1. Produkt musi wspierać systemy operacyjne: Ubuntu Desktop 18.04 LTS 64-bit, Red Hat Enterprise Linux 7 64-bit.
2. Produkt musi posiadać obsługę środowisk pulpitu GNOME,KDE,XFCE.
3. Produkt musi posiadać wsparcie dla dystrybucji 64-bitowych.
4. Wersja programu musi być tylko w języku angielskim.
5. Pomoc produktu musi być w języku polskim oraz angielskim.
6. Produkt nie może posiadać graficznego interfejsu.
7. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
8. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
9. Wbudowana technologia do ochrony przed rootkitami.
10. Skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
11. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
12. Skanowanie plików spakowanych i skompresowanych.
13. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
14. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji
15. programu.
16. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
17. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
18. Aktualizacje modułów analizy heurystycznej.
19. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody

heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Administrator musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.

20. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
21. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych
22. zagrożeń mają być w pełni anonimowe.
23. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
24. Aktualizacja systemu antywirusowego ma być dostępna z Internetu, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
25. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
26. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają
27. wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
28. Program ma umożliwiać importowanie oraz eksportowanie ustawień lokalnie oraz zdalnie za pomocą dedykowanego narzędzia.
29. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego
30. dystrybutora autoryzowanego przez producenta programu.

- **Ochrona urządzeń mobilnych opartych o system Android**

Ochrona antywirusowa:

1. Ochrona plików w czasie rzeczywistym.
2. Ochrona przed atakami typu „phishing”.
3. Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
4. Aplikacja musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
5. Ochrona proaktywna wykrywająca nieznane zagrożenia.
6. W przypadku wykrycia zagrożenia użytkownik ma otrzymać odpowiednie powiadomienie.
7. Aplikacja musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia.
8. Aplikacja musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

Skanowanie na żądanie:

9. Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji.
10. Informacje o skanowaniu mają być przechowywane w plikach dziennika.
11. Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania.
12. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia.

Ochrona przed kradzieżą:

13. Administrator ma mieć możliwość skonfigurowania zaufanej karty SIM.
14. Dodanie zaufanej karty SIM ma się odbyć w oparciu o kartę wprowadzoną w danym urządzeniu lub w oparciu o wprowadzony ręcznie numer IMSI karty SIM.
15. W przypadku kradzieży urządzenia, Administrator ma mieć możliwość wysłania 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.

Polityka ustawień:

16. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej:
    a. połączenie Wi-Fi,
    b. GPS,
    c. usługi lokalizacyjne,
    d. pamięć,
    e. roaming danych,
    f. roaming połączeń,
    g. nieznane źródła,
    h. tryb debugowania,
    i. komunikacja NFC,
    j. szyfrowanie pamięci masowej,
    k. urządzenie zrootowane.

Kontrola aplikacji:

17. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.
18. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.
19. Blokowanie aplikacji musi być możliwe w oparciu o:
    a. nazwę aplikacji,
    b. nazwę pakietu,
    c. kategorię sklepu Google Play,
    d. uprawnienia aplikacji,
    e. pochodzenie aplikacji z nieznanego źródła.

Zabezpieczenia urządzenia:

20. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej:
    a. minimalny poziom zabezpieczeń i złożoność blokady ekranu,
    b. maksymalną dopuszczaną liczbę błędnych prób odblokowania,
    c. odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie,
    d. czas, po którym automatycznie nastąpi blokada ekranu,
    e. ograniczenie dostępu do kamery wbudowanej w urządzenie.

Aktualizacje sygnatur:

21. Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.
22. Aplikacja ma mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje sygnatur co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.
23. Aplikacja ma posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją.

Konfiguracja i zdalne zarządzanie:

24. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne.
25. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.
26. Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych.
27. Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna.
28. Wdrożenie urządzenia mobilnego z poziomu konsoli zarządzającej musi się odbyć co najmniej na jeden z trzech możliwych sposobów:
    a. za pomocą kodu QR,

b. za pomocą unikatowego łącza,
c. za pomocą wiadomości e-mail,

29. W ramach aktywacji za pomocą kodu QR musi istnieć możliwość aktywacji w trybie właściciela urządzenia (Android Enterprise Device Owner).

- **Ochrona serwera - Linux**

Architektura rozwiązania

1. Skaner antywirusowy i antyspyware.
2. Skanowanie plików, plików spakowanych i archiwów samorozpakowujących.
3. Oprogramowanie musi działać w architekturze bazującej na technologii mikro-serwisów.
4. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów oprogramowania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
5. Oprogramowanie musi posiadać wbudowany mechanizm typu ,,watchdog". Monitoruje on tzw. stan zdrowia poszczególnych mikro-serwisów i automatycznie przeładowuje je w przypadku wykrycia zakłóceń w pracy mikro-serwisu.
6. Architektura rozwiązania musi pozwalać na uruchamianie poszczególnych mikro-serwisów, tylko na czas realizacji funkcjonalności przez nie realizowanych, co pozwala w znaczącym stopniu ograniczyć wykorzystanie zasobów systemu operacyjnego.
7. Oprogramowanie antywirusowe musi wspierać wieloprocesorową i wielordzeniową architekturę, w celu zapewnienia maksymalnego zwiększenia wydajności.
8. Oprogramowanie antywirusowe musi być wyposażone w moduł ochrony systemu plików w czasie rzeczywistym. Moduł nie może wymagać instalowania jakichkolwiek dodatkowych komponentów w systemie operacyjnym. Wszystkie komponenty muszą być instalowane w systemie, podczas instalacji z dostarczonego instalatora binarnego.
9. Silnik ochrony systemu plików w czasie rzeczywistym musi stanowić dodatkowy moduł jądra systemu Linux i musi być dodawany do jądra, podczas procesu instalacji oprogramowania antywirusowego.
10. Ochrona systemu plików w czasie rzeczywistym musi być zapewniona nieprzerwanie od uruchomienia produktu i obejmuje skanowanie zarówno dysków lokalnych jak i zmapowanych dysków sieciowych.
11. Silnik skanujący musi działać wyłącznie z wykorzystaniem 64-bitowej architektury.
12. Oprogramowanie musi być w pełni zgodne z modułem SELinux, pracującym zarówno w trybie ,,Permissive" jak i ,,Enforcing".
13. Oprogramowanie podczas procesu instalacji, musi dodawać i konfigurować własne polityki modułu SELinux, które są kompatybilne z następującymi dystrybucjami systemów Linux: Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Centos 6, Centos 7.
14. Wszystkie mechanizmy bezpieczeństwa oprogramowania muszą wspierać system informowania o zagrożeniach w czasie rzeczywistym. System ten pozwala na weryfikowanie reputacji plików oraz procesów i identyfikację nowych i nieznanych zagrożeń.
15. Skaner systemu plików w czasie rzeczywistym musi działać dla operacji obsługi plików, dla co najmniej takich operacji jak: dostęp do pliku, utworzenie (zapisanie) pliku.
16. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

17. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
18. Oprogramowanie musi być wyposażone we własny wiersz polecenia (CLI). Polecenia muszą być odpowiedzialne co najmniej za: skanowanie na żądanie, konfigurację mechanizmów bezpieczeństwa, uruchamianie aktualizacji, przeglądanie logów aplikacji, konfigurację graficznego interfejsu użytkownika, obsługę kwarantanny plików.
19. Rozwiązanie musi wspierać system plików zamontowany z flagą ,,noexec".
20. Oprogramowanie musi pozwalać na uruchamianie zadań skanowania działających ,,w tle", z możliwością ustawienia dla nich niskiego priorytetu.
21. Zadania skanowania nie mogą zmieniać znacznika dostępu do plików.

Interfejs graficzny:

1. Produkt musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna musi działać w oparciu o dynamicznie generowaną zawartość tworzoną z wykorzystaniem następujących technologii: React/Node.js, HTML5.
3. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
4. Lokalna konsola administracyjna musi zapewniać bezpieczne połączenie działające w oparciu
   o protokół HTTPS.
5. Lokalna konsola administracyjna musi umożliwiać uruchomienie jej, na wskazanym porcie TCP.
6. Logowanie do lokalnej konsoli administracyjnej musi być realizowane, poprzez podanie danych w postaci nazwy użytkownika i zdefiniowanego dla niego hasła.
7. Administrator systemu musi mieć możliwość zdefiniowania dodatkowych kont użytkowników,
   w lokalnej konsoli administracyjnej.
8. Lokalna konsola administracyjna musi zapewniać funkcjonalność zweryfikowania stanu licencji
   i informacji na jej temat.
9. Z poziomu lokalnej konsoli administracyjnej musi być możliwość zarządzania, wbudowanym modułem menadżera kwarantanny.
10. Lokalna konsola administracyjna musi zapewniać możliwość przełączenia wersji językowej konsoli, na etapie logowania. Lokalna konsola administracyjna musi posiadać interfejs, co najniej języku: polskim, angielskim.

Skanowanie sieciowych systemów plików:

1. Oprogramowanie antywirusowe musi pozwalać na skanowanie plików składowanych i obsługiwanych przez zewnętrzne rozwiązania obsługi danych typu NAS / SAN.
2. Oprogramowanie antywirusowe nie może wymagać instalacji jakichkolwiek dodatkowych modułów na rozwiązaniach typu NAS / SAN, a skanowanie plików musi się odbywać wyłącznie w oparciu o protokół ICAP.
3. Rozwiązanie musi umożliwiać zmianę domyślnego portu protokołu ICAP.
4. Oprogramowanie antywirusowe, do celów skanowania plików na rozwiązaniach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

Instalacja:

1. Oprogramowanie musi wspierać mechanizm instalacji zdalnej.
2. Oprogramowanie antywirusowe musi być wyposażone w mechanizm automatycznej

aktualizacji komponentów programu.

3. Oprogramowanie musi wspierać następujące systemy operacyjne: RedHat Enterprise Linux (RHEL) 6 64-bit, RedHat Enterprise Linux (RHEL) 7 64-bit, CentOS 6 64-bit, CentOS 7 64-bit, Ubuntu Server 16.04 LTS 64-bit, Ubuntu Server 18.04 LTS 64-bit, Debian 9 64-bit, SUSE Linux Enterprise Server (SLES) 12 64-bit, SUSE Linux Enterprise Server (SLES) 15 64-bit

Licencjonowanie

1. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
2. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.

- **Ochrona serwera Windows**

1. Wsparcie dla systemów: Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012.
2. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
5. Wbudowana technologia do ochrony przed rootkitami i exploitami.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu
10. kontekstowym.
11. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
12. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
13. Możliwość skanowania dysków sieciowych i dysków przenośnych.
14. Skanowanie plików spakowanych i skompresowanych.
15. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
16. Aplikacja powinna wspierać mechanizm klastrowania.
17. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    b. tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku
    wykrycia aktywności w systemie,
    c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    d. 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,

e. tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie
podejrzanych zdarzeniach.

19. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
20. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
21. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
22. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
23. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
24. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze.
25. 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.
26. Funkcja 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.
27. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
28. 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.
29. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
30. Program musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
31. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
32. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
33. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
34. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
35. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
36. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
37. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
38. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
39. 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.

40. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
41. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
42. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e- mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
43. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
44. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
45. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
46. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
47. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
48. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
49. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji.
50. 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.
51. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
52. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
53. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
54. 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.
55. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
56. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.

57. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
58. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
59. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
60. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
61. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
62. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
63. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
64. Aplikacja musi wspierać skanowanie magazynu Hyper-V.
65. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów.
66. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania.
67. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
68. Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”.
69. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
70. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.
71. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
72. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
73. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
74. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
75. Program musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.
76. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
77. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
78. Program musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.

- **Administracja zdalna**
    1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019 oraz systemach Linux.
    2. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.
    3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego

serwera bazy danych MS SQL i MySQL.

4. Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.
5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
6. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
7. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
8. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.
9. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.
10. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.
11. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.
12. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
13. Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym.
14. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
15. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
16. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
17. Serwer administracyjny musi posiadać wsparcie dla „VDI" oraz „Golden Master Image".
18. Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.
19. Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.
20. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
21. Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
22. Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS.
23. Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP.
24. Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11.
25. Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap.
26. Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.
27. Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.
28. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
29. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification
30. Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.

31. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.
32. Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS.
33. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
34. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
35. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
36. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania.
37. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
38. Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.
39. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.
40. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
41. Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.
42. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
43. Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.
44. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
45. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
46. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
47. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.
48. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.
49. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania

serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.

50. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
51. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użycie parametrów instalacyjnych.
52. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
53. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
54. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
55. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
56. 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.
57. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.
58. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
59. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
60. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.
61. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
62. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
63. Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta.
64. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
65. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
66. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
67. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.
68. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
69. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.
70. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może

zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF, CSV oraz PS.

71. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
72. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
73. Powiadomienia mailowe mają być wysyłane w formacie HTML.
74. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.
75. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
76. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
77. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
78. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użycie klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.
79. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
80. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
81. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
82. Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.
83. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
84. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
85. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.
86. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.
87. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.
88. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.
89. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.
90. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.
91. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych.
92. Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault).
93. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez

konieczności przypisywania ich do konkretnych polityk.

94. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).
95. Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.

Ad. I.c. Licencja na oprogramowanie ochrony serwera poczty

Oprogramowanie do ochrony ruchu sieciowego w ramach serwera pocztowego, o funkcjonalności minimum:

- zaoferowany system musi:
    1. zapewniać ochronę zarówno poczty przychodzącej jak i wychodzącej,
    2. zapobiegać próbom spoofingu, phisingu i spyware,
    3. zabezpieczać przed atakami typu DoS
    4. zabezpieczać pocztę wychodzącą, w skład której wchodzi ochrona antywirusowa, kontrola ilości wysłanych wiadomości przez użytkownika,
    5. zapewniać ochronę przed atakami typu DHA.
- ponadto system musi udostępniać następujące funkcjonalności:
    1. W ramach ważnego serwisu administrator ma możliwość zainstalowania skanera antywirusowego dla MS Exchange 2003/2007/2010.
    2. Możliwość ustawiania progów na podstawie punktacji przypisanej przez algorytmy modułu antyspamowego dla wiadomości przychodzących, wg której wiadomości mogą być blokowane, przesyłane do kwarantanny lub oznaczane jako spam.
    3. Możliwość ustawiania progów na podstawie punktacji przypisanej przez algorytmy modułu antyspamowego dla wiadomości wychodzących, wg której wiadomości mogą być blokowane lub przesyłane do kwarantanny.
    4. Analiza odcisku palca wiadomości (fingerprint), pozwalająca na zweryfikowanie wiadomości przychodzącej z bazą odcisków wiadomości zawierających spam, stworzonej przez producenta.
    5. Analiza obrazów dołączonych do wiadomości przy pomocy skanera OCR (Optical Character Recognition).
    6. Weryfikacja adresów URL zawartych w wiadomości z bazą danych znanych adresów URL zawierających spam. Możliwość blokowania, oznaczania, przenoszenia do kwarantanny takich wiadomości spamowych.
    7. możliwość korzystania z filtrów Bayesa.
    8. Możliwość określania maksymalnej ilości połączeń z danego adresu IP w zdefiniowanym przez administratora przedziale czasu. Ustawienie dotyczy zarówno poczty wychodzącej jak i przychodzącej.
    9. Możliwość określania maksymalnej ilości wysłanych wiadomości od danego nadawcy w zdefiniowanym przez administratora przedziale czasu. Ustawienie dotyczy poczty wychodzącej.
    10. Możliwość zdefiniowania adresów email wyłączonych ze sprawdzania maksymalnej ilości wysyłanych wiadomości w zdefiniowanym przez administratora przedziale czasu.
    11. Możliwość ustawienia kwarantanny dla każdego użytkownika.
    12. Możliwość nadania uprawnień użytkownikom do zmiany własnych ustawień:
        a. włączenie/wyłączenie kwarantanny,
        b. włączenie/wyłączenie skanowanie antyspamowego,
        c. zmiany języka i częstotliwości wysyłanych powiadomień kwarantanny,
        d. dodawania adresów do osobistej białej/czarnej listy,
        e. zmiany ustawień osobistych filtru Bayes'.
    13. Możliwość ustawienia częstotliwości wysyłania powiadomienia do użytkownika o nowych wiadomościach przychodzących przeniesionych do kwarantanny: codziennie, raz w tygodniu lub nigdy.

14. Możliwość ustawienia częstotliwości wysyłania powiadomienia do użytkownika o nowych wiadomościach wychodzących od tego użytkownika przeniesionych do kwarantanny: codziennie, co tydzień, natychmiast lub nigdy.
15. Możliwość ustawienia ilości miejsca na dysku przeznaczonej na kwarantannę dla poczty wychodzącej.
16. Możliwość zdefiniowania w przypadku poczty wychodzącej jak długo wiadomości będą przechowywane w kwarantannie.
17. Uwierzytelnianie nadawcy wiadomości na podstawie SPF (Sender Policy Framework).
18. Uwierzytelnianie nadawcy wiadomości na podstawie mechanizmu DKIM (Domain Keys).
19. Zapobieganie niepożądanym wiadomościom bounce z wykorzystaniem metody oznaczania nagłówków wiadomości.
20. Możliwość korzystania z dowolnych zewnętrznych baz RBL.
21. Zapewniać dostęp do baz reputacyjnych producenta, które zawierają listę znanych spamerów.
22. Możliwość zdefiniowania wykluczeń ze skanowania antyspamowego dla wiadomości wychodzących/przychodzących ze określonego adresu IP lub zakresu adresów IP.
23. Możliwość zdefiniowania akcji dla wiadomości przychodzących w przypadku gdy wiadomości zostały wysłane z określonego adresu IP lub określonej podsieci. Dostępne akcje w tym przypadku to: blokowanie, poddanie kwarantannie lub oznaczenie wiadomości jako spam.
24. Możliwość zdefiniowania białej listy domen, subdomen.
25. Możliwość zdefiniowania czarnej listy domen, subdomen. Wiadomości przychodzące z tych domen/subdomen mogą być blokowane, oznaczone jako spam lub przenoszone do kwarantanny.
26. Możliwość określenia dla jakich domen chronionych poczta wychodząca będzie szyfrowana przy pomocy protokołu TLS.
27. Możliwość określenia domen chronionych, dla których poczta wychodząca będzie przekierowana na inny serwer pocztowy.
28. Możliwość określenia dla jakich adresów email poczta wychodząca będzie szyfrowana przy pomocy protokołu TLS.
29. Możliwość określenia adresów email, dla których poczta wychodząca będzie przekierowana na inny serwer pocztowy.
30. Możliwość blokowania wiadomości pochodzących z konkretnego kraju, w tym: Argentyna, Brazylia, Chile, Chiny, Kolumbia, Niemcy, Włochy, Rosja, Turcja.
31. Możliwość tworzenia reguł pozwalających na blokowanie, przesyłanie do kwarantanny lub oznaczenia wiadomości jako spam wiadomości pochodzących z danego hosta.
32. Produkt powinien rozróżniać co najmniej 11 różnych zestawów znaków, różnych narodowości używanych do kodowania wiadomości mailowych. Wiadomości posiadające takie znaki mogą być blokowane, przesłane do kwarantanny lub oznaczone jako spam.
33. System ma umożliwiać korzystanie użytkownikom z dodatkowego pluginu do aplikacji Microsoft Outlook i Lotus Notes.
34. Możliwość konfiguracji ilości dni przechowywania wiadomości w kwarantannie użytkownika.

35. Możliwość uruchomienia SMTP over TLS zarówno dla połączeń wychodzących jak i przychodzących.
36. Możliwość wymuszenia zgodności protokołu SMTP z RFC 821.
37. Możliwość blokowania wiadomości które nie używają FQDN (fully-qualified domain name) w polu 'From' adresu.
38. Kontrola zawartości załączników po:
    a. typie pliku, co najmniej następujące typy: MS Access, MS Excel, MS Word, Adobe PDF, MS PowerPoint, Windows exe, Windows Script. Skaner sprawdza również archiwa pod kątem obecności zdefiniowanych typów pliku,
    b. nazwie pliku lub rozszerzenia pliku, definiowane przez administratora,
    c. typie MIME pliku, definiowane przez administratora zgodnie ze standardem RFC.
39. Dostępne akcje w przypadku kontroli załączników wiadomości mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą:
40. Poczta przychodząca: blokowanie, przeniesienie do kwarantanny,
41. Poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie, przekierowanie na inny serwer.
42. Dostępne akcje w przypadku spakowanych, zabezpieczonych hasłem załączników wiadomości mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą:
43. Poczta przychodząca: blokowanie, przeniesienie do kwarantanny,
44. Poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie, przekierowanie na inny serwer.
45. Możliwość tworzenia reguł, przy pomocy wyrażeń regularnych filtrujących wiadomości po temacie, nagłówku i treści wiadomości. Możliwość tworzenia takich reguł zarówno dla wiadomości przychodzącej jak i wychodzącej. Dostępne akcje mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą:
46. Poczta przychodząca: blokowanie, przeniesienie do kwarantanny, oznaczenie wiadomości, dodanie do białej listy,
47. Poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie wiadomości, dodanie do białej listy, przekierowanie na inny serwer.
48. Minimum 4 predefiniowane, stworzone przez producenta reguły poczty wychodzącej, filtrujące wiadomości po temacie, nagłówku i treści wiadomości.
49. System ma zapewniać skanowanie antywirusowe poczty przychodzącej przy pomocy minimum 3 różnych silników antywirusowych działających jednocześnie.
50. Weryfikacja odcisku wiadomości lub wirusa z bazą danych producenta, jeżeli informacje na temat tej wiadomości lub wirusa nie zostały odnalezione w lokalnej bazie.
51. System ma mieć możliwość przywrócenia poprzednio zainstalowanej bazy sygnatur wirusów.
52. System ma mieć możliwość przywrócenia poprzednio zainstalowanej bazy sygnatur antyspamowych.
53. System ma być konfigurowany za pomocą graficznego interfejsu dostępnego przez przeglądarkę internetową.
54. Interfejs administratora ma być dostępny co najmniej w języku polskim.
55. Możliwość określenia czy administratorzy mają dostęp do interfejsu dostępnego przez przeglądarkę tylko poprzez protokół https.

56. System ma mieć możliwość integracji z usługami katalogowymi LDAP oraz Active Directory przynajmniej do weryfikacji docelowych odbiorców przychodzących przesyłek pocztowych.
57. System ma mieć możliwość skonfigurowania wirtualnych adresów IP do fizycznej karty sieciowej.
58. System ma mieć możliwość konfigurowania tras statycznych.
59. System ma mieć możliwość przeprowadzenia diagnostyki poprzez interfejs graficzny przy użyciu narzędzi takich jak: ping, telnet, dig, tcpdump, traceroute.
60. System ma mieć możliwość uruchomienia bezpiecznego, szyfrowanego połączenia z działem wsparcia technicznego producenta na życzenie administratora.
61. System ma mieć możliwość tworzenia kopii zapasowej konfiguracji, ustawień wszystkich lub wybranych użytkowników.
62. Kopie zapasowe mają być tworzone na żądanie lub eksportowane zgodnie z harmonogramem na zdefiniowany serwer ftp i smb.
63. Możliwość określenia maksymalnej liczby plików kopii zapasowej przechowywanej na serwerze ftp i smb.
64. Możliwość tworzenia kopii zapasowej baz danych filtrów Bayesa, dla całego systemu lub dla poszczególnych użytkowników.
65. Możliwość skonfigurowania adresu email, na który będą przesyłane kopie każdej wiadomości przychodzącej lub wychodzącej.
66. System ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog).
67. W czasie trwania gwarancji zamawiający musi mieć prawo do wykonywania aktualizacji oprogramowania (ang. firmware upgrade).
68. W czasie trwania gwarancji zamawiający musi mieć dostęp do wsparcia technicznego dystrybutora/producenta świadczonego w dni robocze od poniedziałku do piątku w godzinach 8:00-18:00.

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów co najmniej do dnia 31/03/2023.
System musi być objęty serwisem gwarancyjnym producenta przez okres co najmniej do 31/03/2023. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.