**Załącznik nr 1A do SIWZ**

**Dostawa i uruchomienie systemu firewall oraz rozwiązania DLP wraz z niezbędnymi licencjami.**

1. Wymagania techniczne dla klastra urządzeń typu Next Generation Firewall – 2 sztuki urządzeń pracujących w klastrze w trybie active-active wraz z niezbędnym systemem zarządzania.

Każde z dostarczonych urządzeń systemu bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. W ramach postępowania dostawca powinien dostarczyć klaster niezawodnościowy dwóch urządzeń zapewniających poniższe funkcjonalności:

1. Urządzenie musi mieć możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów chroniących systemu.

2. Urządzenie musi zapewniać monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

3. Urządzenie musi posiadać możliwość agregacji linków i równoważenia obciążenia połączeń przy użyciu różnych dostawców łącz internetowych.

4. Urządzenie musi posiadać możliwość agregacji i równoważenia obciążenia pomiędzy tunelami VPN zestawianych przy wykorzystaniu różnych dostawców łącz internetowych.

5.  Urządzenie musi zapewniać monitoring stanu realizowanych połączeń VPN.

6.  Urządzenie realizujące funkcję Firewall musi dawać możliwość pracy w jednym z dwóch trybów: routera z funkcją NAT lub transparentnym.

7.  Urządzenie realizujące funkcje Firewall musi dysponować minimum 8 portami 10/100/1000BASE-TX z możliwością rozbudowy sprzętowej do co najmniej 12 portów 10/100/1000BASE-TX.

8. Urządzenie musi zapewniać możliwość tworzenia min. 100 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.

9.  Urządzenie w zakresie Firewall'a musi obsługiwać nie mniej niż 5 milionów jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę

10.  Urządzenie musi zapewniać przepustowość Firewall'a na poziomie nie mniej niż 10Gbps dla pakietów maksymalnie UDP 1518 bajtów.

11.  Urządzenie musi zapewniać wydajność szyfrowania AES-256: nie mniej niż 150Mbps.

12. Urządzenie w ramach dostarczonego systemu ochrony musi realizować wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:

a.      Firewall - zapora ogniowa klasy Stateful lnspection,

b.      połączenia szyfrowane lPSec VPN,

c.      ochrona typu lntrusion Prevention System [IPS],

d.      kontrola pasma oraz ruchu (QoS, Traffic shaping),

e.      Kontrola aplikacji oraz rozpoznawanie ruchu P2P,

f.       Możliwość analizy ruchu szyfrowanego protokołem SSL,

13.   Urządzenie musi zapewniać wydajność skanowania ruchu w celu ochrony przed atakami (IPS) na poziomie min. 1 Gbps przy czym skanowanie musi obejmować całe pakiety.

14.   Urządzenie w zakresie realizowanych funkcjonalności VPN, musi zapewniać nie mniej niż:

a.     Tworzenie połączeń w topologii Site-to-Site oraz Client-to-Site,

b.      Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności,

c.      Praca w topologii Hub and Spoke oraz Mesh,

d.      Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF,

e.      Obsługa mechanizmów: IPSec NAT Traversal, XAuth,

15.   Urządzenie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPV2, OSPF, BGP. Protokoły routingu powinny mieć możliwość funkcjonowania w ramach terminowanych na urządzeniu połączeniach IPSec VPN.

16.  Urządzenie musi zapewniać możliwość rozbudowy do obsługi min. 5 oddzielnych logicznych instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a.

17.  Urządzenie musi zapewniać możliwość translacji adresów NAT adresu źródłowego i NAT adresu docelowego.

18.  Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).

19. Urządzenie musi zapewniać możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ, Internal, External.

20. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 6500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.

21.  Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie analizy całych pakietów do warstwy 7 modelu ISO/OSI, a nie bazując jedynie na wartościach portów TCP/UDP lub innych właściwościach warstw 3 i 4 modelu ISO/OSI.

22.  Automatyczne aktualizacje sygnatur ataków i aplikacji.

23. Urządzenie musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:

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 SecurlD) w oparciu o zewnętrzne bazy danych,

d. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single-Sign-On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.

24. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać certyfikat iCSA lub równoważny dla funkcjonalności Firewall, IPS.

25.  Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

**Serwisy i licencje**

Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres co najmniej **12 miesięcy**, dotyczy to zwłaszcza funkcjonalności: Intrusion Prevention System i Application Control.

**Gwarancja oraz wsparcie**

System powinien być objęty serwisem producenta przez okres co najmniej **12 miesięcy**. Czas naprawy lub dostarczenia urządzenia zastępczego nie powinien być dłuższy niż 10 dni.

**Wdrożenie**

Wymagane jest zainstalowanie i skonfigurowanie klastra urządzeń w środowisku Zamawiającego.

***Urządzenie do zarządzania i monitoringu – 1 zestaw***

Zamawiający wymaga dostarczenia centralnego systemu zarządzania urządzeniami typu Next Generation Firewall wraz z niezbędnymi licencjami do zarządzania klastrem urządzeń Firewall (łącznie 2 urządzenia).

Elementy systemu bezpieczeństwa odpowiedzialne za zarządzanie i monitoring mają umożliwiać centralizację procesów zarządzania wszystkimi funkcjonalnościami elementów realizujących funkcje bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

W ramach systemu logowania i raportowania dostawca powinien dostarczyć spójny system monitorujący, gromadzący logi i generujący raporty na podstawie danych ze wszystkich elementów systemu bezpieczeństwa.

Platforma powinna dysponować predefiniowanym zestawem przykładów raportów, dla których administrator systemu będzie mógł modyfikować parametry prezentowania wyników.

System centralnego logowania i raportowania powinien być dostarczony w postaci komercyjnej platformy sprzętowej lub programowej.

W ramach centralnego systemu logowania i raportowania powinny być realizowane przynajmniej poniższe funkcjonalności:

1. Konfigurowalne opcje powiadamiania o zdarzeniach jak. email, SNMP.

2. Podgląd logowanych zdarzeń w czasie rzeczywistym.

3. Możliwość generowania raportów w zakresie wszystkich funkcjonalności bezpieczeństwa realizowanych przez system - na żądanie oraz w trybie cyklicznym, w postaci popularnych formatów min: PDF, HTML. Raporty powinny obejmować zagadnienie dotyczące całej sfery bezpieczeństwa.

4. Zastosowane systemy logowania powinny umożliwiać cykliczny eksport zgromadzonych logów do zewnętrznych systemów przechowywania danych w celu ich długo okresowego składowania.

**Gwarancja:**

System powinien być objęty serwisem producenta przez okres co najmniej **12 miesięcy**. Czas naprawy lub dostarczenia urządzenia zastępczego nie powinien być dłuższy niż 10 dni.

1. Wymagania techniczne dla systemu ochrony poczty elektronicznej

System ochrony poczty elektronicznej ma zapewnić ochronę przed spamem i wiadomościami email zawierającymi kod złośliwy oraz dodatkowe funkcjonalności, opisane poniżej, w zakresie kontroli i ochrony poczty elektronicznej Zamawiającego.

System powinien być dostarczony w postaci oprogramowania możliwego do zainstalowania na dowolnym serwerze spełniającym minimalne wymagania techniczne producenta zapewnionym przez Zamawiającego.

**Szczegółowe wymagania dotyczące funkcjonalności systemu i zakresu usług.**

*Wymagania ogólne.*

1. System ochrony poczty elektronicznej musi obsługiwać **nie mniej niż 400 użytkowników Zamawiającego.**

2. W ramach dostawy systemu ochrony należy zapewnić licencje na oprogramowanie ochronne.

3. W razie potrzeby rozbudowy systemu pod kątem wydajności dostarczone licencje muszą umożliwiać wdrożenie kolejnych gateway’i pocztowych opartych na appliance i/lub maszynach wirtualnych VMware, bez konieczności zmiany licencji, dokupowania ich lub zakupu dodatkowego oprogramowania.

*Wymagania szczegółowe.*

1. Interfejs zarządzający dostępny przez przeglądarkę internetową i połączenie https bez użycia maszyny wirtualnej Java.

2. GUI interfejsu zarządzania musi być wyposażone w konfigurowany pulpit (dashboard), na którym znajduje się podsumowanie najważniejszych parametrów Gateway’a i wyników ochrony poczty.

3. Musi istnieć możliwość zdefiniowania wielu kont administratorów i przypisania im uprawnień do wykonywania tylko pewnych czynności administracyjnych (co najmniej ograniczenie dostępu tylko do konfiguracji polityk bez możliwości zmian konfiguracji sieciowej, ograniczenie dostępu tylko do modułu raportowania, ograniczenie dostępu do konfiguracji szyfrowania poczty).

4. Konta administratorów można tworzyć lokalnie w systemie oraz korzystać z zewnętrznych usług katalogowych dostępnych przez protokoły Radius i Kerberos.

5.Oprogramowanie dostarczanego rozwiązania musi umożliwiać centralne zarządzanie wieloma gateway’ami działającymi w klastrze, jak i niezależnie bez konieczności zakupu dodatkowych licencji lub oprogramowania.

6. System musi posiadać wbudowane raportowanie, bez konieczności stosowania dodatkowego oprogramowania i zewnętrznych serwerów.

7. Moduł raportujący powinien posiadać gotowe, predefiniowane szablony raportów oraz powinien umożliwiać tworzenie raportów spersonalizowanych.

8. Raporty mają być generowane na żądanie i okresowo, według zdefiniowanego harmonogramu.

9. Musi być możliwe zapisanie Raportu, co najmniej w formacie PDF, HTML, TXT.

10. Musi być możliwe automatyczne wysłanie raportu mailem pod wskazany adres.

11. Interfejs zarządzający musi umożliwiać wizualizację przebiegu transakcji SMTP i przejścia wiadomości przez poszczególne filtry ochronne Gateway’a.

12. Interfejs zarządzający musi umożliwiać administratorowi zarządzanie wiadomościami przechowywanymi w lokalnej kwarantannie.

*Wymagania dotyczące implementacji sieciowej.*

13. Rozwiązanie powinno umożliwiać wdrożenie gateway’a pocztowego w trybie proxy aplikacyjnego (mail relay), routera (transparent router) oraz transparent bridge.

14. W każdym z trybów pracy powinna być zachowana taka sama funkcjonalność ochrony poczty przed spam i kodem złośliwym.

15. Rozwiązanie musi posiadać wbudowane mechanizmy budowy klastra wysokiej dostępności (HA) oraz współdzielącego ruch dla rozłożenia obciążenia między urządzenia wchodzące w skład klastra.

16. Rozwiązanie ma działać w warstwie sieciowej (gateway poczty elektronicznej) i musi obsługiwać co najmniej protokoły SMTP i POP3, przy czym musi być możliwe określenie portów na jakich działają te protokoły.

17. Gateway’e muszą umożliwiać wysyłanie wiadomości SNMP, syslog oraz powiadomień w formie poczty elektronicznej dla zdefiniowanych zdarzeń.

18. Gateway’e muszą posiadać wbudowane wydajne mechanizmy ograniczania skutków ataków typu Denial of Service (DoS) z wykorzystaniem poczty elektronicznej co najmniej takie, jak:

a.Określenie maksymalnego czasu pomiędzy komendami SMTP.

b.Określenie minimalnej przepustowości przesyłania danych.

c.Określenie maksymalnej liczby tzw. trywialnych komend SMTP

d.Określenie maksymalnej ilości odbiorców wiadomości.

e.Określenie maksymalnej długości połączenia SMTP.

f.Określenie maksymalnej długości części domenowej adresu.

g.Stosowanie technik zapobiegających przed atakami Directory Harvest, gdzie można zdefiniować ile procentowo odbiorców musi być niepoprawnych w stosunku do wszystkich by zablokować połączenie od nadawcy.

19. System ma zapewniać ochronę anti-relay.

20. System musi mieć możliwość ochrony przed spamem przez użycie graylistingu.

*Wymagania dotyczące tworzenia polityk*

21. Gateway musi posiadać wbudowany mechanizm przeciwdziałania wyciekowi danych (filtr DLP).

22. Filtr DLP musi działać na tej samej platformie, co pozostałe funkcjonalności ochronne i nie może wymagać zastosowania dodatkowych licencji lub oprogramowania.

23. Musi istnieć możliwość zarejestrowania (zindeksowania) chronionych dokumentów bezpośrednio poprzez GUI Gateway’a pocztowego.

24. Poza zarejestrowaniem chronionych dokumentów musi być także możliwe określenie chronionych treści na podstawie słów kluczowych, fraz, wyrażeń regularnych i słowników (w tym słowników tworzonych samodzielnie przez Zamawiającego) zawierających słowa, frazy i wyrażenia regularne.

25. Moduł DLP musi posiadać predefiniowane reguły wykrywające dane dotyczące polskich danych, co najmniej numerów: PESEL, NIP, dowodów osobistych, REGON oraz paszportów.

*Wymaganai dotyczące obsługi szyfrowania poczty*

26. Każdy z Gateway’ów pocztowych musi umożliwiać szyfrowanie poczty elektronicznej korzystając z technologii:

1. B2B (Gateway – Gateway) – szyfrowanie w tunelu TLS/SSL pomiędzy gateway’ami oraz między gateway’em a serwerem pocztowym, szyfrowanie S/MIME, szyfrowanie PGP.
2. B2U (Gateway – User) – szyfrowanie wiadomości pocztowej w taki sposób, aby jej odczytanie możliwe było po uwierzytelnieniu się odbiorcy na portalu web dostępnym poprzez HTTPS. Portal Web musi być obsługiwany bezpośrednio przez Gateway pocztowy.
3. System musi umożliwiać elastyczną definicję wiadomości, które mają być szyfrowane (co najmniej zależnie od odbiorcy, domeny pocztowej, treści wiadomości, określonych słów kluczowych w temacie wiadomości, specyficznych nagłówków dodanych do wiadomości pocztowej).
4. System musi umożliwiać importowanie certyfikatów i ustalenie w polityce, który z nich zostanie użyty do uwierzytelnienia tuneli TLS/SSL z poszczególnymi odbiorcami (na podstawie ich domeny pocztowej i adresacji IP).

*Wymagania dotyczące wykrywania kodu złośliwego.*

27. Gateway pocztowy musi być wyposażony w skaner anti-malware (AM) pochodzący od tego samego producenta, co całe oferowane rozwiązanie.

28. Skaner AM musi wykorzystywać dzienne, automatyczne aktualizacje baz sygnatur antywirusowych.

29. Musi istnieć możliwość określenia częstotliwości i harmonogramu aktualizacji silnika AM i baz sygnatur.

30. Skaner AM musi posiadać mechanizm wykrywający nowe zagrożenia w technologii „in the cloud” za pomocą serwisów reputacyjnych posiadanych przez producenta rozwiązania.

31. W razie wykrycia podejrzanego kodu/pliku i braku definicji w lokalnym pliku sygnatur anty-wirusowych, skaner AM musi mieć możliwość wysłania zapytania do centralnej bazy prowadzonej przez producenta rozwiązania o to czy dany plik/kod jest już znany i zakwalifikowany jako zagrożenie.

a. Zależnie od wyniku zapytania, skaner AM musi mieć możliwość podjęcia takiej samej reakcji jak w przypadku wykrycia zagrożenia na podstawie lokalnego pliku sygnatur.

32. Skaner AM musi wykrywać i blokować oprogramowanie szpiegujące oraz wykrywać próby ataków typu PHISHING.

33. Skaner AM musi umożliwiać blokowanie skryptów, apletów Java oraz ActiveX.

34. Oprócz skanera anti-malware (AM) pochodzącego od tego samego producenta, co całe oferowane rozwiązanie powinien być dostępny inny silnik anti-malware innego producenta. Silnik ten powinien być dostarczany w ramach głównej licencji – bez dodatkowych kosztów.

*Wymagania dotyczące ochrony anty-spamowej*

35. Gateway pocztowy musi zapewniać także ochronę przed spamem – powinien być wyposażony w moduł anty-spam (AS) pochodzący od tego samego producenta, co całe oferowane rozwiązanie.

36. Skaner AS musi działać w oparciu o system oceny prawdopodobieństwa wystąpienia spamu bazujący na regułach aktualizowanych przez producenta.

37. Aktualizacja reguł musi odbywać się na bieżąco kilka razy na godziną, a co najmniej raz dziennie.

38. Skaner AS musi współpracować z serwerami AD i LDAP pozwalając na stworzenie dokładnej polityki skanowania zależnie od adresu email, grupy użytkowników w AD/LDAP, domeny pocztowej, zakresu adresów IP.

39. System AS musi obsługiwać białe i czarne listy (blacklist i whitelist) definiowane przez administratora oraz samodzielnie przez końcowych użytkowników (odbiorców poczty).

40. System AS musi obsługiwać serwery RBL prowadzone przez producenta rozwiązania. Musi być także możliwe definiowanie dodatkowych źródeł RBL przez administratora systemu.

41. System AS musi wykrywać i blokować ataki typu directory harvest.

42. System AS musi obsługiwać technologie graylist, SPF oraz Sender ID.

43. System AS musi chronić przed spamem generowanym za pomocą mechanizmu potwierdzania problemów z doręczeniem przesyłki (NDR).

44. System AS musi posiadać filtr reputacyjny badający domenę i adres IP, z których nadana została wiadomość oraz zawartość przesyłaną w email:

a. Musi być możliwe takie skonfigurowanie polityki ochrony anty-spam, aby już sam wynik z serwisu reputacyjnego (niska reputacja nadawcy) powodował odrzucenie email lub skierowanie go do kwarantanny.

b. Musi być także możliwe uwzględnienie wyników z serwisu reputacyjnego w całościowej ocenie prawdopodobieństwa wykrycia spam i podejmowanie decyzji o losie email na podstawie końcowego wyniku analizy, po przejściu email przez inne filtry analizujące wiadomość.

45. System powinien umożliwiać rozpoznawanie URL’i w treści wiadomości i filtrować wiadomość i URL’ami o złej reputacji. Kontrola reputacji URL powinna być badana w momencie dostarczania wiadomości oraz w momencie kliknięcia URL’a przez użytkownika w kliencie pocztowym w czasie rzeczywistym.

46. Musi być możliwe zdefiniowanie różnych akcji podejmowanych po wykryciu spamu zależnie od określonego przez system prawdopodobieństwa wykrycia spam.

*Obsługa kwarantanny*

47. Gateway musi umożliwiać zapisanie wiadomości do kwarantanny przechowywanej lokalnie, a także na zewnętrznym serwerze.

48. Decyzja o zapisaniu wiadomości do kwarantanny musi wynikać z definicji działania poszczególnych filtrów: anti-malware, anti-spam, DLP i weryfikacji treści.

49. Administrator Gateway’a ma mieć możliwość dostępu do lokalnej kwarantanny na Gateway’u bezpośrednio z interfejsu GUI.

50.Musi być możliwe zdefiniowanie maksymalnego czasu przechowywania wiadomości w kwarantannie.

51. Gateway musi umożliwiać automatyczne wysyłanie mailem powiadomień o wiadomościach zatrzymanych w kwarantannie do ich oryginalnych odbiorców.

**Serwisy i licencje**

Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji systemu na okres co najmniej 12 miesięcy (w formie licencji typu dożywotniego lub subskrypcji na minimum 12 miesięcy).

**Gwarancja oraz wsparcie**

System powinien być objęty serwisem producenta przez okres co najmniej 12 miesięcy.

**Wdrożenie**

Wymagane jest zainstalowanie i skonfigurowanie systemu w środowisku Zamawiającego na urządzeniach zapewnionych przez Zamawiającego.

1. Wymagania dla systemu filtracji i ochrony ruchu web

System filtracji i ochrony ruchu web ma zapewnić blokowanie dostępu użytkownikom do niepożądanych treści i stron www na podstawie ich kategorii, ochronę przed wirusami i oprogramowaniem szpiegującym oraz phishingiem, uwierzytelnienie i autoryzację użytkowników nawiązujących połączenia do stron www, a także zapewniać ochronę w trybie odwrotnego proxy (tzw. reverse proxy).

System powinien być dostarczony w postaci oprogramowania możliwego do zainstalowania na dowolnym serwerze spełniającym minimalne wymagania techniczne producenta.

**Szczegółowe wymagania dotyczące funkcjonalności systemu i zakresu usług.**

*Wymagania funkcjonalne*

1. System ochrony WEB ma obsługiwać nie mniej niż 400 użytkowników Zamawiającego.
2. System ochrony WEB musi realizować funkcje proxy aplikacyjnego (7 warstwa modelu OSI/ISO) co najmniej dla następujących protokołów:
   1. HTTP
   2. HTTPS
   3. FTP
   4. RTSP (streaming)
   5. IM (instant messaging) –Jabber
3. System ochrony WEB musi także (równocześnie z funkcją proxy) pozwalać na skonfigurowanie trybu pracy odwrotnego proxy (reverse-proxy) dla protokołów http i https.
4. System WEB musi realizować ochronę anty-malware z użyciem minimum 2 niezależnych silników anty-malware jednocześnie, w tym
   1. co najmniej jeden nie może pochodzić od tego samego producenta co producent systemuu ochrony WEB,
   2. musi istnieć możliwość zmiany ilości silników anty-malware (jeden lub dwa) zaangażowanych w analizę ruchu dla różnych podsieci IP Zamawiającego i dla różnych kategorii stron WWW
5. Rozwiązanie do ochrony anty-malware musi korzystać, poza lokalnymi definicjami zagrożeń (sygnatury), także z centralnej bazy zagrożeń udostępnianej przez producenta rozwiązania WEB, do której dostęp jest realizowany w razie potrzeby, automatycznie poprzez Internet.
6. Poza ochroną opartą na sygnaturach znanych ataków, rozwiązanie musi także posiadać mechanizmy ochrony umożliwiające:
7. Wdrożenie proaktywnej ochrony przed nowymi atakami „zero day“ poprzez analizę zachowania złośliwego kodu w co najmniej: ActiveX, Windows Executables, DLLs, JAVA Applications, Java Script, Visual Basic Scripts, VBA Macros.
8. Wykrywanie co najmniej następujących znamion kodu złośliwego: Shell Code, Exploit Detection, blokowanie, poprzez wykrywanie akcji jaka byłaby wykonana przez kod na końcowym komputerze (np. dostęp do procesu COM), ataków Buffer Overflow.
9. Skanowanie i wyodrębnianie obiektów wbudowanych wewnątrz dokumentów typu: Generic XML, SOAP, PDF, MS Office, MS OpenXML.
10. System musi mieć możliwość usuwania z kodu HTML następujących podejrzanych obiektów: Visual Basic Script, JavaScript, Java.
11. Możliwość automatycznego wykrywania połączeń typu streaming i wykluczania ich z analizy anty-malware.
12. System ochrony WEB musi umożliwiać zaawansowane funkcje filtracji ruchu, co najmniej:
13. filtracja na podstawie sygnatur co najmniej 500 różnych aplikacji działających w oparciu o obsługiwane protokoły web – na przykład takie aplikacje jak: Skype, TeamViewer, Google Docs, Facebook, itp.
14. filtracja reklam w trakcie odwiedzania strony przez użytkownika, bez blokowania dostępu do strony (banery, formularze, grafika o określonych rozmiarach).
15. filtracja komend w HTTP oraz FTP (np APPEND, HEAD).
16. filtracja różnych rodzajów mediów na podstawie tzw. Magic Byte (video, application, music, zip, itp.).
17. Autentykacja użytkowników
18. System ochrony WEB musi umożliwiać autentykowanie użytkowników nawiązujących połączenie Web.
19. Autentykacja użytkowników musi być realizowana w sposób transparentny (bez dodatkowego żądania uwierzytelnienia przez użytkownika w czasie nawiązywania połączenia) i dodatkowo, jako opcja w konfiguracji, z wyświetleniem zapytania o dane użytkownika.
20. System ochrony WEB musi obsługiwać lokalną bazę danych o użytkownikach i ich grupach oraz zewnętrzne bazy danych – co najmniej: Microsoft AD 2003/2008 (NTLMv2 i Kerberos), LDAP, Radius, Novell eDirectory.
21. System ochrony WEB musi umożliwiać autentykację z wykorzystaniem certyfikatów cyfrowych i plików cookie.
22. Musi istnieć możliwość jednoczesnego skorzystania z więcej niż jednej metody uwierzytelnienia użytkownika, na zasadzie: jeśli użytkownik nie został odnaleziony w pierwszej bazie użytkowników, sprawdź w kolejnej, jeśli nie został odnaleziony w kolejnej, sprawdź w następnej, itd.”.
23. Podłączenie systemu ochrony WEB do domeny Active Directory dla przeprowadzania zintegrowanej autentykacji użytkowników nie może wymagać instalacji dodatkowych komponentów sprzętowych lub aplikacji w środowisku Zamawiającego.
24. System ochrony WEB musi umożliwiać także zdefiniowanie akcji dla użytkowników, którzy nie mogli być zautentykowani (np. dla osób-gości czasowo podłączonych do sieci Zamawiającego, którzy nie należą do jego baz użytkowników). Taką akcją musi być dla przykładu zapewnienie im dostępu do określonych stron WWW i określonych kategorii stron WWW.
25. System ochrony WEB musi realizować cache dla ruchu web, przy czym informacje z cache muszą być automatycznie weryfikowane pod kątem zagrożeń oraz oznakowane i usuwane w momencie pojawienia się nowych sygnatur anti-malware.
26. Filtracja dostępu do stron i serwisów Web na podstawie predefiniowanych i aktualizowanych przez producenta systemu ochrony WEB baz URL i adresów IP:
27. System ochrony WEB musi korzystać zarówno z lokalnej (załadowanej na urządzeniu), aktualizowanej okresowo bazy adresów URL i IP jak również z centralnej bazy prowadzonej przez producenta ochrony WEB, dostępnej z urządzeń przez Internet automatycznie w czasie rzeczywistym.
28. Baza adresów URL i IP musi umożliwiać skorzystanie w polityce filtracji ruchu z co najmniej 100 predefiniowanych przez producenta ochrony WEB kategorii.
29. System musi umożliwiać samodzielną, lokalną zmianę przypisania stron WWW do kategorii przez administratora w konfiguracji rozwiązania.
30. System musi umożliwiać określenie polityki, w której określeni użytkownicy/grupy użytkowników będą mieli ograniczony czasu spędzany na stronach z danej kategorii URL.
31. System musi umożliwiać określenie polityki, w której określeni użytkownicy/grupy użytkowników będą mieli ograniczoną ilość danych ściąganych ze stron z danej kategorii URL.
32. System musi umożliwiać ograniczanie pasma ruchu do i z serwera www dla określonych użytkowników, kategorii, adresów IP z sieci Zamawiającego.
33. System ochrony WEB musi umożliwić skorzystanie z serwisu reputacyjnego określającego ryzyko korzystania z danego serwera/strony web, prowadzonego przez producenta ochrony WEB:
34. w czasie nawiązywania połączenia musi być możliwe automatyczne zweryfikowanie reputacji strony i na tej podstawie blokowanie dostępu do niej, nawet jeśli taki dostęp jest dozwolony w ramach danej kategorii URL.
35. System ochrony WEB musi zapewnić skanowanie ruchu pod kątem zagrożeń w tunelach szyfrowanych https/ssl:
36. funkcja ta musi być realizowana w taki sposób, aby ruch zaszyfrowany nie opuszczał urządzenia celem zeskanowania.
37. urządzenia muszą deszyfrować, a następnie szyfrować połączenie (tryb man-in-the-middle).
38. system musi umożliwić analizę poprawności certyfikatów serwera użytych do zestawienia połączenia https/ssl. W razie wykrycia niepoprawnego certyfikatu (np. z niezaufanego CA, samodzielnie podpisanego (self signed), itp.) system musi umożliwić automatyczne zablokowanie połączenia.
39. system musi umożliwiać wykluczenia wskazanych przez administratora adresów stron WWW i kategorii URL ze skanowania https/ssl.
40. Konfiguracja polityki działania systemu ochrony WEB:
41. Konfiguracja systemu musi umożliwiać tworzenie reguł wykorzystujących w dowolnych kombinacjach co najmniej takie parametry jak:
    * Adres docelowy URL
    * Adres docelowy IP (reverse DNS lookup)
    * Indywidualny nagłówek żądania http (np. X-Forwarded-For)
    * Rodzaj agenta nawiązującego połączenie (np. rodzaj przeglądarki web)
    * Adres IP klienta nawiązującego połączenie
    * Nazwy użytkownika i grup użytkowników
    * Poziom reputacji strony
    * Kategorię do jakiej należy strona www
    * Aplikację jaka jest wykorzystywana do łączenia się ze serwerem web
    * Czas (w tym np. przez określenie okresu: między godziną X a godziną Y)
    * Kraj gdzie jest zlokalizowany serwer Web (dla określenia kraju nie może być wykorzystywana tylko nazwa domeny, ale także adres IP serwera).
42. System ochrony WEB musi umożliwiać podłączenie do sieci Zamawiającego w różny sposób, bez konieczności zakupu dodatkowych licencji lub modułów sprzętowych i oprogramowania. Muszą być obsługiwane co najmniej następujące tryby pracy systemu:
43. Jednoznacznie wskazane proxy (tzw. explicit proxy)
44. Z wykorzystaniem protokołu Cisco WCCP
45. Z wykorzystaniem protokołu IFP (Internet Filtering Protocol)
46. Z wykorzystaniem protokołu ICAP
47. Transparent bridge
48. Transparent router
49. System ochrony WEB musi umożliwić także integrację z zewnętrznym systemem przeciwdziałania wyciekowi danych (DLP) poprzez protokół ICAP.
50. System ochrony WEB musi umożliwiać wyświetlenie dla użytkownika powiadomienia o podjętej przez system akcji (np. wykrycie zagrożenia).
51. System ochrony WEB musi umożliwić elastyczne logowanie informacji w zewnętrznych systemach zarządzania logami i SIEM z wykorzystaniem SNMP i Syslog oraz musi umożliwić wysłanie wiadomości email w razie wystąpienia wcześniej zdefiniowanego zdarzenia (np. wykrycie wirusa).
52. System musi umożliwiać definiowanie własnych rodzajów logów zawierających różne kombinacje parametrów połączenia obsługiwanego przez System.
    1. Musi istnieć możliwość zdefiniowania warunków, kiedy dany rodzaj logu jest zapisywany przez system – co najmniej: zapis logu tylko w sytuacji zablokowania połączenia przez Systemem, zapis logu tylko jeśli połączenie jest nawiązywane z określonych adresów IP, zapis logów tylko pod warunkiem, że połączenie jest inicjowane przez określonego użytkownika (na podstawie danych z jego autentykacji).
53. Zarządzanie systemem ochrony WEB:
54. Zarządzanie systemem ochrony WEB powinno być możliwe za pomocą przeglądarki WWW i protokołu HTTPS,
55. System powinien umożliwiać tworzenie wielu kont administratorów lokalnie lub wykorzystanie kont z AD, LDAP i Radius,
56. System musi umożliwiać szczegółowe określenie uprawnień poszczególnym administratorom, w tym ograniczenie ich uprawnień do określonych reguł polityki działania systemu (np. tylko możliwość włączania i wyłączania kategorii URL dla określonej grupy użytkowników).

*System raportujący*

System ochrony WEB musi zapewnić szczegółowy wgląd w statystyki ruchu, stan pracy urządzeń, wykrytych zagrożeń. Dane te powinny być prezentowane zarówno bezpośrednio z konsoli zarządzającej systemem jak również w postaci dedykowanego systemu raportującego (*off-box raporting*).

Dedykowany system raportujący (off-box) musi być tego samego producenta co system ochrony WEB. System raportujący powinien realizować co najmniej:

* 1. Centralne gromadzenie logów i danych na temat połączeń do Internetu z urządzeń wchodzących w skład systemu ochrony WEB.
  2. Zarządzanie systemem raportującym musi się odbywać przez przeglądarkę WWW i protokół HTTPS.
  3. Gromadzenie danych w bazie danych SQL, przy czym musi być możliwe użycie wbudowanej bazy danych SQL w system raportujący (dostarczonej wraz z systemem raportującym) lub zewnętrznej bazy, co najmniej MS SQL

**Serwisy i licencje**

Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji systemu na okres **co najmniej 12 miesięcy** (w formie licencji typu dożywotniego lub subskrypcji **na minimum 12 miesięcy**).

**Gwarancja oraz wsparcie**

System powinien być objęty serwisem producenta przez okres **co najmniej 12 miesięcy**.

**Wdrożenie**

Wymagane jest zainstalowanie i skonfigurowanie systemu w środowisku Zamawiającego na urządzeniach zapewnionych przez Zamawiającego.

1. Wymagania techniczne dla systemu do całkowitego szyfrowania dysków

System powienien umożliwiać całkowite szyfrowanie dysków komputerów stacjonarnych i przenośnych (laptop). Proces oraz polityka szyfrowania powinna być egzekwowana przez agenta instalowanego lokalnie na szyfrowanym zasobie. Wymagane jest aby system udstępniał możliwość centralnego zarządzania polityką szyfrowania dla objętych procesem szyfrowania zasobów.

**Szczegółowe wymagania dotyczące funkcjonalności systemu i zakresu usług.**

*Wymagania funkcjonalne*

1. Rozwiązanie ma zapewnić szyfrowanie **dla minimum 400 stacji** użytkowników.
2. Rozwiązanie musi zapewnić szyfrowanie danych na poziomie dysku w sposób transparentny dla systemu operacyjnego i użytkownika, z funkcjonalnością autentykacji użytkownika bezpośrednio po uruchomieniu komputera (przed wystartowaniem właściwego systemu operacyjnego - tzw. pre-boot authentication, PBA).
3. System szyfrowania musi zapewniać centralne zarządzanie, w oparciu o centralną bazę danych, gdzie przetrzymywane są informacje o użytkownikach, kluczach i politykach szyfrowania niezbędne do uzyskania dostępu do danych zaszyfrowanych na stacji w sytuacji awaryjnej.
4. Oprogramowanie szyfrujące na stacjach użytkowników musi komunikować się z serwerem zarządzającym w bezpieczny sposób (transmisja szyfrowana z obustronną autentykacją) z wykorzystaniem protokołów opartych na TCP/IP, które umożliwiają połączenie przez sieci routowane.
5. Musi istnieć możliwość określenia czy szyfracji mają podlegać wszystkie partycje dysku, czy tylko partycja bootowalna (z której startuje właściwy system operacyjny) czy tylko partycje „niebootowalne”. Musi też istnieć możliwość określenie dowolnej konfiguracji partycji do zaszyfrowania.
6. Rozwiązanie musi wspierać obsługiwać co najmniej AES 256 jako algorytm szyfrowania danych.
7. Rozwiązanie musi samodzielnie wykrywać czy procesor chronionego komputera obsługuje sprzętowe wsparcie szyfracji (Intel AES-NI) i automatycznie wykorzystywać tą funkcjonalność podczas szyfracji/deszyfracji danych.
8. Autentykacja użytkownika w PBA ma być możliwa z wykorzystaniem hasła i nazwy użytkownika, ale także z użyciem tokenów, smart cards różnych producentów oraz biometrii.
9. System powinien umożliwiać samodzielne wgranie na token indywidualnego klucza użytkownika, który umożliwia dostęp do danych zaszyfrowanych na dysku.
10. System powinien pozwalać na użycie modułu TPM 2.0 w celu uniknięcia potrzeby preautentykacji użytkowników.
11. Musi być zapewniona obsługa autentykacji użytkowników w trybie pre-boot authentication z wykorzystaniem systemu PKI (kart inteligentnych przechowujących certyfikaty użytkowników). Wymagana jest obsługa co najmniej Microsoft PKI.
12. System powinien pobierać użytkowników z AD oraz dać możliwość ręcznej definicji użytkowników. System musi umożliwiać wskazanie, który użytkownik i grupa mają prawo używać komputer i uzyskać dostęp do zaszyfrowanych danych.
13. Użytkownicy i grupy użytkowników przypisywani do komputerów muszą być synchronizowani z domeną Microsoft AD.
14. Usunięcie użytkownika w serwerze usług katalogowych AD powinno skutkować automatycznym usunięciem lub zablokowaniem użytkownika w serwerze zarządzającym systemem szyfrowania.
15. System musi umożliwiać automatyczne dodanie do listy uprawnionych użytkowników, użytkowników z domeny AD, którzy wcześniej korzystali z komputera (logowali się do niego).
16. Zmiany hasła użytkownika na jednej maszynie muszą być automatycznie powielane i synchronizowane na pozostałych komputerach, do których jest przypisany ten użytkownik.
17. Rozwiązanie musi umożliwiać pracę w trybie single sign-on – po zalogowaniu się w trybie pre-boot authentication użytkownik nie musi już logować się po raz kolejny do systemu Windows, jego dane są automatycznie przekazywane do procesu logowania Windows.
18. System szyfrowania musi umożliwiać centralną kontrolę jakości haseł używanych przez użytkowników przez określenie minimum: długości hasła, zawartości hasła (znaki numeryczne i alfanumeryczne, symbole, itp.), historię stosowanych haseł, wymuszenie zmiany hasła przez użytkownika.
19. System musi zapewnić centralne przechowywanie kluczy użytych do szyfracji danych i możliwość odzyskania zaszyfrowanych danych z ich wykorzystaniem w sytuacji awarii.
20. System musi umożliwiać zresetowanie hasła zapomnianego przez użytkownika dla trybu PBA bez konieczności otwierania połączenia zdalnego do komputera użytkownika.
21. Każdy komputer musi posiadać swój unikalny klucz wykorzystywany do szyfrowania danych na dysku.
22. Oprogramowanie szyfrujące musi kontynuować pracę po niespodziewanym zaniku zasilania, bez wpływu na możliwość zaszyfrowania i odszyfrowania danych.
23. Stacje i użytkownicy mają synchronizować zmiany w politykach szyfrowania i parametrach systemu bez konieczności interwencji administratora.
24. Instalacja oprogramowania na stacji powinna się odbywać bez interwencji użytkownika.
25. System przed rozpoczęciem szyfrowania powinien sprawdzić, czy na komputerze nie znajduje się oprogramowanie niekompatybilne.
26. System musi umożliwiać zalogowanie się do głównego systemu operacyjnego z pominięciem pre-boot authentication pod warunkiem wyrażenia na to zgody przez administratora systemu.
27. System powinien umożliwiać generowanie raportów dotyczących co najmniej: stanu szyfracji systemu (stacja nie zaszyfrowana, stacja zaszyfrowana, stacja w trakcie szyfracji), wersji działającego oprogramowania szyfracji, przypisanych do stacji użytkowników.
28. System szyfrowania powinien zapewnić obsługę co najmniej następujących systemów operacyjnych: Windows XP, Windows Vista, Windows 7 oraz Windows 8.
29. Producent oferowanego rozwiązania do szyfracji systemów Windows musi oferować także analogiczne rozwiązanie do szyfracji laptopów Apple MAC, zarządzane z tej samej konsoli zarządzania co produkty dla MS Windows. Produkt dla szyfracji Apple MAC nie jest przedmiotem aktualnego postępowania.
30. Musi istnieć dobrze zdefiniowany proces odzyskiwania danych w sytuacjach awaryjnych: zagubienie hasła i nazwy użytkownika, po uszkodzeniu systemu operacyjnego, po uszkodzeniu systemu szyfrowania.
31. Obsługa mechanizmu resetowania/odzyskiwania hasła i tokenu użytkownika w rozwiązaniu do szyfracji danych nie może wymagać podłączenia stacji do sieci firmowej.
32. Musi istnieć możliwość samodzielnego zresetowania hasła przez użytkownika w trybie pre-boot authentication w oparciu o udzielenie odpowiedzi na wcześniej zdefiniowane pytania, bez konieczności podłączenia stacji do sieci firmowej.
33. System szyfracji dysków musi obsługiwać dyski twarde z wbudowanym mechanizmem szyfracjji sprzętowej w standardzie OPAL.
34. Po automatycznym wykryciu takiego dysku, oferowane rozwiązanie musi przekazać obsługę szyfracji do wbudowanego mechanizmu w dysku.
35. Rozwiązanie musi być przetestowane przez producenta z minimum czteroma różnymi dyskami OPAL. Producent powinien zapewnić dostęp do listy kompatybilności dysków z OPAL.

**Serwisy i licencje**

Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji systemu na okres **co najmniej 12 miesięcy** (w formie licencji typu dożywotniego lub subskrypcji **na minimum 12 miesięcy**).

**Gwarancja oraz wsparcie**

System powinien być objęty serwisem producenta przez okres **co najmniej 12 miesięcy**.

**Wdrożenie**

Wymagane jest zainstalowanie i skonfigurowanie systemu w środowisku Zamawiającego na urządzeniach zapewnionych przez Zamawiającego.

1. Wymagania techniczne dla systemu szyfrowania plików, folderów i urządzeń przenośnych.

System powienien umożliwiać szyfrowanie plików, folderów i urządzeń przenośnych. Wymagane jest aby system udstępniał możliwość centralnego zarządzania polityką szyfrowania dla objętych procesem szyfrowania zasobów.

Szczegółowe wymagania dotyczące funkcjonalności systemu i zakresu usług.

*Wymagania funkcjonalne*

1. Rozwiązanie ma zapewnić obsługę nie mniej niż 400 stacji użytkowników.
2. Rozwiązanie musi szyfrować:
   1. pliki i katalogi w ramach systemu operacyjnego i udziałów sieciowych udostępnianych przez serwery sieciowe

b. dane kopiowane na urządzenia zewnętrzne USB oraz CD/DVD

1. Rozwiązanie powinno umożliwiać tworzenie na USB szyfrowanych kontenerów.
2. Rozwiązanie powinno umożliwiać integrację z podsystemem ochrony przed wyciekiem danych DLP (opisanym poniżej) co najmniej poprzez umożliwienie sterowania szyfracją plików kopiowanych na nośniki USB z poziomu polityki DLP.
3. System szyfracji plików i folderów musi być możliwy do wdrożenia niezależnie od rozwiązania do szyfracji dysków.
4. System szyfrowania musi zapewniać centralne zarządzanie, w oparciu o centralną bazę danych i aplikację tą samą, jaka jest używana do zarządzania systemami DLP i szyfracją dysków.
5. W centralnym systemie zarządzania mają być generowane i przetrzymywane klucze używane do szyfracji oraz definiowane szczegółowe polityki działania szyfrowania plików i folderów.
6. Oprogramowanie szyfrujące na stacjach użytkowników musi komunikować się z serwerem zarządzającym w bezpieczny (transmisja szyfrowana z obustronną autentykacją) sposób z wykorzystaniem protokołów opartych na TCP/IP.
7. Rozwiązanie musi wykorzystywać algorytm AES 256 do szyfracji danych.
8. Rozwiązanie musi umożliwiać centralnie, z serwera zarządzającego:
9. Określenie typów plików, jakie mają być szyfrowane przez wskazanie procesu jakie je tworzy i rozszerzeń plików
10. Określenie maksymalnego rozmiaru pliku jaki ma być szyfrowany
11. Określenie jaki klucz ma być użyty do szyfracji danych
12. Określenie czy i jakim kluczem mają być szyfrowane dane kopiowane na nośniki USB i CD/DVD
13. Określenie czy pliki jakie znajdują się już wcześniej na nośniku USB mają być także zaszyfrowane po zastosowaniu polityki szyfracji czy raczej pozostawione bez zmian
14. Rozwiązanie musi umożliwiać centralne zdefiniowanie katalogów na dyskach lokalnych komputerów użytkowników, które mają być zaszyfrowane:
15. Musi być możliwe określenie, jaki klucz ma być użyty do szyfracji
16. Musi być możliwe używanie zmiennych systemowych Windows do określenia jaki folder ma być zaszyfrowany – w szczególności dla określenia folderów typu „Moje Dokumenty”
17. Musi być możliwa zmiana widoku ikony folderu i zaszyfrowanych plików w sposób identyfikujący, że są one zaszyfrowane
18. Musi być zapewniona możliwość szyfrowania danych na sieciowych udziałach dyskowych Windows przez to samo oprogramowanie, które służy do szyfrowania plików i katalogów lokalnie:
19. Szyfracja udziałów sieciowych nie może wymagać instalowania oprogramowania na serwerach plików
20. Musi istnieć możliwość współdzielenia plików zaszyfrowanych bez konieczności ich deszyfracji.
21. System musi zapewnić centralne przechowywanie kluczy użytych do szyfracji danych i możliwość odzyskania zaszyfrowanych danych z ich wykorzystaniem w sytuacji awarii.
22. System musi zapewniać centralne przydzielenie tych samych kluczy używanych do szyfracji do wielu użytkowników i grup użytkowników z Active Directory (AD).
23. Niezależnie od centralnie przydzielonych wspólnych kluczy dla grupy użytkowników, każdy użytkownik musi posiadać także unikalny klucz, przypisany do niego automatycznie, wykorzystywany do szyfrowania plików i katalogów.
24. System szyfrowania powinien zapewnić obsługę następujących systemów operacyjnych: Windows XP, Windows Vista, Windows 7 oraz Windows 8.
25. System szyfrowania plików i katalogów powinien zapewnić obsługę następujących systemów plików:
26. dla systemów lokalnych: NTFS, FAT32, FAT16, CDFS, UDFS,
27. dla sieciowych udziałów dyskowych: NTFS, FAT32, FAT16.

**Serwisy i licencje**

Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji systemu na okres **co najmniej 12 miesięcy** (w formie licencji typu dożywotniego lub subskrypcji **na minimum 12 miesięcy).**

**Gwarancja oraz wsparcie**

System powinien być objęty serwisem producenta przez okres **co najmniej 12 miesięcy.**

**Wdrożenie**

Wymagane jest zainstalowanie i skonfigurowanie systemu w środowisku Zamawiającego na urządzeniach zapewnionych przez Zamawiającego.

1. Wymagania techniczne dla systemu ochrony przed wyciekiem danych

System ochrony przed wyciekiem danych powinnien składać się z centralnego elementu zarządzajacego oraz elementów końcowych instalowanych na stacjach klienckich objętych procesem monitorowania i ochrony przed wyciekiem danych. Centralny system zarządzający powinien umożliwiać tworzenie i dystrybucję polityk oraz dostarczać funkcji raportujących.

**Szczegółowe wymagania dotyczące funkcjonalności systemu i zakresu usług.**

*Wymagania funkcjonalne*

1. Rozwiązanie ma zapewnić obsługę co najmniej 400 stacji użytkowników.
2. Rozwiązanie musi składać się z centralnego serwera zarządzającego, konsoli zarządzania opartej na przeglądarce web oraz modułu DLP instalowanego na komputerach użytkowników.
3. Rozwiązanie musi umożliwiać zdalną instalację oprogramowania klienckiego DLP.
4. System musi znakować czasowo wszystkie zdarzenia napływające do serwera.
5. System powinien umożliwiać klasyfikację istotnych danych podlegających ochronie w oparciu o minimum:
6. miejsce pochodzenia danych (katalog sieciowy),
7. zawartość pliku z danymi (słowa, wyrażenia, słowniki ze słowami i wyrażeniami, wyrażenia regularne), przy czym musi być możliwe określenie minimalnej ilości wystąpień słowa/wyrażenia/wyrażenia regularnego w pliku, która powoduje wykonanie klasyfikacji dokumentu jako chronionego,
8. aplikację, która wytworzyła dane i typ pliku zawierający dane,
9. adres URL strony, z której pochodzi (został ściągnięty) dokument,
10. ręczne oznakowanie danych do ochrony, przy czym musi być możliwe określenie jacy użytkownicy i jakie grupy użytkowników z AD mają prawo do ręcznej klasyfikacji,
11. podobieństwa do innych dokumentów poprzez indeksy utworzone z wybranych dokumentów podlegających ochronie (tzw. fingerprint).
12. Klasyfikacja danych powinna być wykonywana dynamicznie przez moduł DLP na stacjach, bez konieczności wykonywania okresowego, masowego znakowania danych.
13. Nazwy znaczników klasyfikacji danych powinny być konfigurowalne przez administratora.
14. Klasyfikacja danych na podstawie lokalizacji pliku, na podstawie aplikacji i na podstawie adresu URL, z którego pochodzi plik musi umożliwiać właściwe działanie reguł reakcji na nieuprawnione postępowanie z takimi plikami bez konieczności otwierania pliku przez moduł DLP i skanowania jego zawartości.
15. Klasyfikacja takiego pliku nie może się zmieniać (w szczególności być gubiona) w przypadku co najmniej zmiany nazwy pliku, zmiany formatu/typu pliku,
16. W przypadku skopiowania fragmentu tak sklasyfikowanego pliku do innego dokumentu, nowy dokument musi dziedziczyć taką samą klasyfikację jak plik oryginalny.
17. Reguły monitorowania wykorzystania danych i blokowania powinny być tworzone w oparciu o znaczniki.
18. Musi istnieć możliwość zawężenia definicji chronionych danych w oparciu o:
19. Rodzaj pliku
20. Rozszerzenie nazwy pliku
21. Meta dane dokumentu – co najmniej: autor, nazwa pliku, data utworzenia, data modyfikacji, szablon użyty do utworzenia dokumentu.
22. Minimalny wymagany zakres działań ochronnych modułu DLP
23. Ochrona wydruków
24. Definiowanie ograniczeń w drukowaniu wskazanych dokumentów sklasyfikowanych jako chronione, w tym możliwość wskazania, który dokument może być drukowany na której drukarce
25. Monitorowanie, blokowanie drukowania danych na wskazanych drukarkach oraz raportowanie takiego zdarzenia obejmujące minimum: nazwę drukarki, nazwę użytkownika, proces, który wysłał dokument do drukowania, IP adres komputera użytkownika, czas zdarzenia
26. Reagować (monitorowanie, blokowanie – zależnie od konfiguracji), gdy
    * 1. dane chronione są kopiowane przez połączenie sieciowe (definiowane jako zakres IP adresów, rodzaj protokołu sieciowego, w tym poprzez określenie nr portów, na jakich odbywa się połączenie)
      2. gdy dane chronione znajdują się w wychodzącym emailu z dokładnością do odbiorcy maila, domeny mailowej
      3. gdy następuje próba dostępu dowolną aplikacją do danych chronionych
      4. gdy następuje próba wysłania danych przez przeglądarkę internetową z dokładnością do domeny i strony web
      5. próba skopiowania danych chronionych przez funkcjonalność Print-Screen, podczas gdy z innych danych (niechronionych) mogą by wykonywane zrzuty ekranowe
      6. próba przeniesienia danych chronionych przez schowek systemowy(clipboard)
      7. próba przeniesienia danych chronionych na urządzenia zewnętrzne (tzw. removable storage)
27. Dostępność różnych rodzajów reakcji modułu DLP na wykryte naruszenie polityki ochrony:
28. Blokowanie akcji (np. zablokowanie wysłania email)
29. Monitorowania akcji (wysłanie alertu i logu do serwera zarządzającego)
30. Powiadomienie użytkownika (wyświetlenie użytkownikowi informacji, że podjęta akcja została zablokowana/ jest monitorowana przez moduł DLP)
31. Zapytanie użytkownika o podanie powodów wykonywania akcji – powód wpisany przez użytkownika musi być zachowany na serwerze zarządzającym
32. Automatyczna szyfracja chronionych plików podczas ich przesyłania na katalog sieciowy lub na dysk zewnętrzny USB – przy czym administrator systemu ma możliwość wskazania jaki klucz zostanie użyty do szyfracji i jakie osoby/grupy użytkowników mają prawo dostępu do klucza i zaszyfrowanych danych
33. Zachowanie dowodów - skopiowanie danych, które spowodowały podjęcie akcji przez moduł DLP na wskazany udział sieciowy (w tym też obrazy wykonanych zrzutów z ekranu). Dane kopiowane na udział muszą być szyfrowane, a dostęp do nich możliwy tylko z konsoli systemu zarządzania
34. Wykrywanie czy dane wysyłane przez email poza organizację są zaszyfrowane lub spakowane z hasłem i blokowanie takiej akcji przez moduł DLP
35. Moduł DLP musi umożliwiać natywne, okresowe przeszukiwanie dysków twardych na stacjach roboczych pod kątem występowania tam plików zawierających ważne dane. W razie wykrycia takiego pliku powinno być możliwe wykonanie akcji:
36. Przesłanie powiadomienia do serwera zarządzającego
37. Przydzielenie do pliku klasyfikatora oznaczającego, że plik ma podlegać ochronie przez moduł DLP
38. Przeniesienie pliku do lokalnej kwarantanny
39. Wykonanie kopii z odnalezionego pliku i skopiowanie jej do wskazanego udziału sieciowego w postaci zaszyfrowanej
40. Skasowanie pliku z dysku
41. Powinna istnieć możliwość uzależnienia działania systemu DLP od stanu stacji roboczej – czy jest ona podłączona do sieci firmowej (tryb on-line) czy pracuje poza nią (tryb off-line).
42. Proces tworzenia polityk dla systemu powinien być uproszczony przez predefiniowane szablony np: numery kart kredytowych, urządzenia USB, itp.

*Wymagania dotyczące raportowania*

1. System zarządzania powinien umożliwić operacje na obiektach typu: komputer, grupa komputerów, użytkownik, grupa użytkowników zsynchronizowanych z MS Active Directory.
2. Konsola zarządzania musi umożliwiać ustawienie polityk per odbiorca lub cała domena.
3. Rozwiązanie powinno generować log zarówno z incydentów bezpieczeństwa określonych w politykach jak i działań administratorów systemu dla celów audytowych.
4. Log musi zawierać user ID, czas zdarzenia, nazwę hosta oraz informacje o zdarzeniu takie jak: nazwa procesu, nazwa reguły, podjęte akcje, itp.
5. System powinien umożliwiać przeglądanie na bieżąco zdarzeń napływających z komputerów objętych ochroną i wspierać generowanie własnych raportów z zebranych danych oraz umożliwiać eksport danych do postaci plików CSV i/lub formatu XML.
6. System powinien umożliwić podgląd statusu wszystkich agentów.
7. Konsola zarządzania powinna mieć możliwość ograniczenia dostępu administracyjnego z podziałem co najmniej na: tylko do odczytu, przeglądanie zdarzeń, pełna administracja.

**Serwisy i licencje**

Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji systemu **na okres co najmniej 12 miesięcy** (w formie licencji typu dożywotniego lub subskrypcji **na minimum 12 miesięcy**).

**Gwarancja oraz wsparcie**

System powinien być objęty serwisem producenta przez okres **co najmniej 12 miesięcy**.

**Wdrożenie**

Wymagane jest zainstalowanie i skonfigurowanie systemu w środowisku Zamawiającego na urządzeniach zapewnionych przez Zamawiającego.

1. Ogólne warunki wdrożenia rozwiązania

Uruchomienie obejmuje instalację oraz konfigurację zgodnie z wymaganiami Zamawiającego. Wykonawca zobowiązany będzie do wykonania migracji z aktualnie posiadanego systemu firewall około 100 reguł filtrowania.

Wymianę wraz z wymaganą rekonfiguracją aktualnego środowiska firewall na zaproponowane w dostawie.

Prace wdrożeniowe wpływające na ciągłość funkcjonowania systemów muszą być wykonane poza godzinami pracy ULC tj 8.15 – 16.15. Czynności nie naruszające pracy systemów mogą być wykonane w godzinach pracy.

Ze względów bezpieczeństwa infrastruktury Zamawiającego szczegółowa charakterystyka posiadanego rozwiązania firewall zostanie przekazana Wykonawcy, z którym zostanie podpisana Umowa na dostawę oraz instalację. Zamawiający szacuje, iż czas potrzebny na migrację to około 4-5 dni roboczych, godzin popołudniowych lub dni wolnych od pracy (soboty). Instalacja będzie miała miejsce w siedzibie zamawiającego.