POWIAT PLESZEWSKI
ul. Poznańska 79, 63-300 Pleszew
tel. 62 74 29 652, faks 62 74 29 665

Załącznik nr 1

Opis przedmiotu zamówienia.

I. SYSTEM ZABEZPIECZENIA DANYCH PRZED WYCIEKIEM INFORMACJI.

Zamawiający wymaga dostawy kompletnego narzędzia do ochrony danych przed wyciekiem, składającego się z komponentów opisanych poniżej. Wymagane jest aby cała funkcjonalność była dostępna w ramach jednej instalacji oferowanego systemu ochrony danych przed wyciekiem ze zintegrowanym systemem klasyfikacji dokumentów. Nie dopuszcza się systemów wyposażonych w zewnętrzne narzędzie do klasyfikacji dokumentów.

1. Funkcjonalność ogólna:

1). Wymagane jest, aby produkt klasyfikował, identyfikował i raportował urządzenia według typu, producenta, modelu i numeru seryjnego. Funkcja ta jest konieczna by usprawnić proces definiowania polityki bezpieczeństwa dla poszczególnych użytkowników oraz grup w organizacjach.

2). Wymaga się, by produkt zaopatrzony był w funkcje zabezpieczające przed aktywnością lokalną użytkowników:

a). odinstalowanie oprogramowania możliwe dzięki hasłu, które zna wyłącznie administrator domenowy;

b). ochrona przed użytkownikami posiadającymi uprawnienia administratora, chcącymi usunąć bądź wyłączyć oprogramowanie;

c). rejestrowanie wszelkich prób manipulacji przez użytkowników (łącznie z usuwaniem logów);

d). wszystkie pliki logów będą zaszyfrowane przed nieautoryzowanym dostępem i próbą skasowania;

e). wszystkie połączenia między aplikacją agencką na stacji roboczej a serwerem zarządzającym będą zaszyfrowane przy użyciu protokołu SSL.

3). Proponowane rozwiązanie musi być kompatybilne z systemem Windows Serwer 2012/2016 oraz Active Directory, które użytkuje Zamawiający . Musi ono oferować proste tworzenie polityk i kojarzenie ich z dowolnymi obiektami Active Directory. Dodatkowo, system musi umożliwiać tworzenie wirtualnych OU (ang. Organization Unit) z możliwością przypisywania do nich obiektów niedomenowych:

a). polityki mogą być powiązane z jednym lub kilkoma obiektami AD:

- ✓ domena
- ✓ jednostka Organizacyjna (OU)
- ✓ grupa
- ✓ użytkownik
- ✓ komputer

4). Polityki muszą być aktualizowane na Klientów bezpośrednio przez serwer zarządzający rozwiązania.

5). Wymagane jest wdrożenie aplikacji agenckiej w postaci pakietów MSI z możliwością dystrybucji tych pakietów co najmniej przez Active Directory GPO lub inne systemy dystrybucji centralnej oprogramowania.

6). Konsola administratora musi być zainstalowana na więcej niż jednym komputerze aby umożliwić administratorom dostęp z kilku różnych lokalizacji.

7). Produkt musi umożliwiać kontrolę następujących portów fizycznych i bezprzewodowych:

a). USB;

b). Firewire;

c). PCMCIA;

d). port szeregowy (Com);

e). port równoległy (LPT);

f). modem;

g). karty SD;

h). bluetooth;

i). WiFi;

j). podczerwień.

8). Produkt musi posiadać funkcję identyfikowania urządzeń poprzez numery seryjne znajdujące się na "białych listach" dopuszczonych urządzeń, takich jak:

a). wymienne urządzenia pamięci masowej;

b). CD/DVD;

c). zewnętrzne dyski twarde;

d). dyskietki;

e). napędy taśmowe;

f). telefony komórkowe;

g). urządzenia oparte o system Android;

h). urządzenia oparte o system iOS;

i). urządzenia oparte o system BlackBerry;

j). urządzenia PDA;

k). Smart Card;

l). urządzenia drukujące;

ł). adaptery sieciowe;

m). urządzenia audio/video;

n). urządzenia interfejsu HID;

o). urządzenia do przetwarzania obrazów.

9). System musi oferować możliwość blokowania wszystkich powyższych typów urządzeń.

10). Proponowane rozwiązanie musi posiadać funkcję blokowania nośników i urządzeń pamięci masowej, takich jak:

a). wymienne urządzenia pamięci masowej (np. pamięć USB);

b). napędy CD/DVD;

c). zewnętrzne dyski twarde;

d). napędy dyskietek;

e). napędy taśmowe;

f). urządzenia interfejsu HID (np. klawiatury, myszki komputerowe);

g). urządzenia drukujące;

h). telefony komórkowe;

i). adaptery sieciowe;

j). urządzenia do przetwarzania obrazów (np. aparaty), urządzenia AV (np. odtwarzacze MP3 i iPody);

k). Karty Smartcard, urządzenia zabezpieczające (np. urządzenia biometryczne).

11). Ponadto, muszą posiadać opcję ustawiania dostępu tylko do odczytu dla wszystkich wymiennych nośników (np. pamięci USB), napędów CD/DVD i napędów dyskietek.

12). Rozwiązanie musi być wyposażone w logi i alerty dostępne dla wdrożenia produktu i zarządzania nim, w tym:

a). szczegółowe logi dotyczące wdrożenia zabezpieczeń na stacjach pracowników, rejestrujące wszystkie zdarzenia z możliwością wygenerowania specjalnego alertu odnośnie danego typu zdarzenia;

b).logowanie działań po stronie klienta obejmujące: zainstalowanie klienta; odinstalowanie klienta; zawieszenie ochrony; wznowienie ochrony; użycie nieprawidłowego hasła użytkownika; nieprawidłowe hasło administratora; próby ingerencji w aplikację kliencką (brakujące zdarzenia, zakończone procesy, nieważna polityka);

c). logowanie działań po stronie serwera obejmujące: aktualizację polityk; nieprawidłową aktualizację polityk; generowanie hasła zatrzymania ochrony; logowanie/wylogowanie administratora; zapisanie polityki; publikację polityki; zmiany administracyjne; zmiany ustawień polityki globalnej; licencje oprogramowania.

d). każde zdarzenie musi umożliwiać tworzenie dodatkowych powiadomień. Alerty wysyłane będą za pośrednictwem poczty email, SNMP lub jako Windows Event Log;

e). dla użytkowników, logowanie musi być zaimplementowanie lokalnie na stacji roboczej. Logi powinny być wysyłane ze stacji do serwera zarządzającego i przechowywane w centralnie dostępnym katalogu.

Na serwerze musi być możliwość automatycznego odszyfrowywania za pomocą klucza systemowego, który przechowywany jest w folderze konfiguracji systemu.

13). Produkt musi zapewniać pełne raportowanie audytowe i alerty wszystkich aktywności, takich jak:

a). podłączenie urządzeń i nośników pamięci na dowolnym porcie;

b). odłączenie urządzeń i nośników pamięci na dowolnym porcie;

c). odczyt/zapis plików z urządzeń pamięci masowej;

d). podłączanie do sieci bezprzewodowych;

e). próby operacji na oprogramowaniu klienckim (różnego rodzaju, wraz ze szczegółami dotyczącymi tych prób);

f). aktualizacje polityk;

g). instalowanie/odinstalowywanie klienta;

h). zawieszenie/wznowienie ochrony;

i). podanie nieprawidłowego hasła;

j). administrator musi posiadać możliwość określenia, które z tych działań mają być ignorowane, wysyłane jako logi lub alerty.

14). Produkt musi posiadać wbudowane i definiowane przez użytkownika raporty graficzne. Musi być wyposażony w system raportowania umożliwiający wysyłane zapytań, które pozwalają na tworzenie logów i alertów według określonych kryteriów.

15). Produkt ma chronić przed urządzeniami typu Keylogger USB i PS/2 poprzez ich wykrywanie i unieszkodliwianie.

16). Produkt musi blokować funkcję auto odtwarzania urządzeń przenośnych.

17). Proponowane rozwiązanie musi również blokować urządzenia USB posiadające wbudowany system operacyjny (np. LiveUSB lub U3) oraz umożliwiać blokowanie działania (np. autostart) w ramach polityki bezpieczeństwa.

18). Produkt musi umożliwiać zapis nazw plików zapisanych na DVD/CD oraz innych urządzeniach przenośnych. Wszystkie pliki zapisywane i odczytywane z CD/DVD, urządzeń przenośnych i zewnętrznych dysków twardych muszą być zalogowane. W logach muszą być zawarte informacje dotyczące zapisanych lub odczytanych plików z urządzeń pamięci masowej, takie jak: czas, komputer, użytkownik, polityka, nazwa, rodzaj i rozmiar pliku, działanie (np. zapis, odczyt).

19).Produkt musi posiadać funkcję szyfrowania zewnętrznych nośników danych. Funkcja ta musi również umożliwiać administratorom szyfrowanie wszystkich danych, które są przesyłane ze stacji roboczych do dopuszczonych nośników danych, takich jak:

a). zewnętrzne dyski twarde;

b). pamięci flash USB;

c). CD/DVD.

20). Rekomendowane rozwiązanie musi posiadać funkcję kontroli operacji i przesyłanych plików zarówno z jak i na przenośne urządzenia USB także podczas pracy offline – poza domeną.

21). Ponadto, produkt musi blokować wszystkie lub tylko wybrane aktywności portów: zezwalanie, blokowanie lub „ograniczanie” użycia jakiegokolwiek lub wszystkich portów komputera w firmie („ograniczanie” oznacza, że blokowane jest użycie portu, chyba że polityka na to pozwoli)

22).Przedstawione rozwiązanie musi współpracować z systemem operacyjnym Microsoft Windows XP, 7, 8, 8.1, 10 zarówno w wersji 32 jak i 64 bitowej oraz Microsoft Windows Server 2008 R2, 2012 R2 i 2016 jako serwer zarządzający.

23). Proponowane rozwiązanie musi wspierać instalację na wirtualnej platformie Vmware lub Hyper-V i być z nią kompatybilne.

24). System musi mieć wbudowaną klasyfikację danych (realizowaną mechanizmami tego samego producenta, na tym samym serwerze co system ochrony) za pomocą poniższych elementów:

a). słowa kluczowe;

b). wzory sygnatur np. numer faktury, numer projektu, numer dokumentu;

c). metadane dokumentów (m.in. autor, data, temat, szablon);

d). typy plików;

e). odciski cyfrowe dokumentów.

25). System musi oferować funkcjonalność wymuszenia klasyfikacji każdego dokumentu przetwarzanego przez użytkownika, bezpośrednio w momencie wystąpienia interakcji między użytkownikiem a danymi.

26). Na podstawie określonej klasyfikacji danych system musi umożliwiać przeszukiwanie lokalnych zasobów komputerów pracowników pod kątem występowania sklasyfikowanych danych.

27). System musi oferować pełne logowanie każdej aktywności użytkownika i umożliwiać raportowanie zebranych informacji w formie graficznej. Produkt musi zapewniać pełne raportowanie i alerty wszystkich aktywności w kanałach komunikacji użytkownika, takich jak:

a). próba wysłania sklasyfikowanych informacji kanałem email;

b). próby udostępnienia sklasyfikowanych informacji przez przeglądarki internetowe w tym (IE, Firefox, Chrome, Opera);

c). próba udostępnienia sklasyfikowanych danych poprzez udziały sieciowe lub przez zasoby chmurowe;

d). próby drukowania danych sklasyfikowanych na drukarkach lokalnych lub sieciowych;

e). próby skopiowania danych sklasyfikowanych na wirtualny zasób (np. maszyna wirtualna uruchomiona w ramach stacji roboczej pracownika).

28). Administrator musi posiadać możliwość określenia, które z tych działań mają być ignorowane, wysyłane jako logi lub alerty.

29). Rozwiązanie musi oferować ochronę danych w kanałach komunikacji, uwzględniając inspekcję danych pod względem klasyfikacji danych (po zawartości dokumentu). Musi uwzględniać monitorowanie i kontrolę takich kanałów komunikacji jak:

a). e-mail;

b). strony internetowe (przeglądarki);

c). wydruki (na drukarkach lokalnych i sieciowych);

d). foldery sieciowe;

e). serwery FTP;

f). komunikatory internetowe;

g).udziały chmurowe;

h). udziały wirtualne;

i). aplikacje do nagrywania płyt;

j). aplikacje do synchronizacji danych z urządzeniami mobilnymi.

30). Oferowane rozwiązanie musi posiadać funkcjonalności szyfrowania danych na dyskach komputerów. Wymagane jest aby taka funkcjonalność działała w ramach już istniejącej instalacji bez konieczności instalowania nowych aplikacji (w tym nowego agenta na stacjach) lub nowego środowiska. Moduł szyfrujący musi być zarządzany z tej samej konsoli co cały system ochrony danych.

31). Wymaga się dostarczenia systemu redundantnego, pozwalającego na uruchomienie co najmniej dwóch serwerów – podstawowego w siedzibie głównej Zamawiającego i zapasowego w centrum zapasowym Zamawiającego. Instalacja wysokiej dostępności musi zapewnić możliwość kontrolowania środowiska ochrony danych przed wyciekiem z systemu zapasowego w przypadku awarii serwera podstawowego.

32). **Zamawiający wymaga dostarczenia 70 licencji wraz ze wsparciem technicznym oraz aktualizacją systemu do najnowszej wersji na okres co najmniej 1 roku od daty dostarczenia rozwiązania.**

33). Oferowana licencja musi być licencją dożywotnią, z możliwością wykupienia corocznie praw do aktualizacji i wsparcia technicznego realizowanego przez producenta.

II. <u>WDROŻENIE I SZKOLENIE - SYSTEM ZABEZPIECZENIA DANYCH PRZED WYCIEKIEM INFORMACJI.</u>

1. Etap I: Przygotowanie instalacji systemu.

1). Wykonawca zobowiązany jest opracować i przedstawić harmonogram prac z podziałem na etapy i ramy czasowe do zatwierdzenia przez Zamawiającego.

2. Etap II: Instalacja w siedzibie Zamawiającego.

1). Implementacja rozwiązania (serwer zarządzający) na bazie przesłanej dokumentacji - na serwerze Zamawiającego (Dell R730 Service Tag: 5DGR1L2) system Windows Server 2016.

2). Implementacja agentów oprogramowania na bazie przesłanej dokumentacji przy wykorzystaniu GPO, przygotowanie plików instalacji i samej polityki GPO po stronie Wykonawcy.

Zamawiający zapewni co najmniej jedną osobę do wsparcia instalacji agentów aby lokalnie nadzorować instalację na stacjach roboczych. Zamawiający odpowiada we własnym zakresie za instalację agentów na sprzęcie, który będzie w wyjątkowych sytuacjach poza domeną.

3). Sprawdzenie integralności instalacji agentów.

4). Weryfikacja komunikacji Klient-Serwer.

5). Sprawdzenie poprawności działania usług oferowanego rozwiązania.

3. Etap III: Konfiguracja systemu.

1). Konfiguracja podstawowych parametrów pracy oprogramowania:

a). ustawienia zachowania agenta;

b). ustawienia backupów logów i kluczy szyfrujących;

c). konfiguracja trybu pracy modułów (general policy).

2). Uruchomienie polityk z zakresu funkcjonalnego oferowanego rozwiązania.

3). Opisanie, zaplanowanie i stworzenie do 6 szczegółowych polityk oferowanego rozwiązania na bazie ustaleń z Zamawiającym (maksymalnie 70 maszyn lub użytkowników we wszystkich politykach), uwzględniając przyjęty zakres ochrony portów i kontroli urządzeń:

a). określenie blokowanych typów urządzeń;

b). stworzenie białej listy urządzeń dopuszczonych do podłączania (nie mniej niż 40 sztuk);

c).stworzenie polityki odpowiedzialnej za kopiowanie danych na nośniki zewnętrzne.

4). Opisanie, zaplanowanie i stworzenie do 4 szczegółowych polityk oferowanego rozwiązania na bazie ustaleń z Zamawiającym (maksymalnie 70 maszyn lub użytkowników we wszystkich politykach), uwzględniając zakres ochrony danych wrażliwych, sklasyfikowanych wcześniej przez Zamawiającego, zawierających:

a). politykę dla ruchu pocztowego;

b). politykę dla przeglądarek.

III. <u>SZKOLENIE - SYSTEM ZABEZPIECZENIA DANYCH PRZED WYCIEKIEM INFORMACJI</u>.

1. Zakres szkolenia z oferowanego rozwiązania - system zabezpieczenia danych przed wyciekiem informacji:

1). Szkolenie 4 osób w siedzibie Zamawiającego, minimum 5 godzin.

Minimalny zakres tematyczny:

a). wprowadzenie w wymogi technologiczne każdego z modułów, instalacji serwera;

b). budowanie polityk bezpieczeństwa

- ✓ ogólne zasady;
- ✓ dobre praktyki.

c). zasady komunikacji Klient – Serwer (Agent – Management Server):

- ✓ wymagania instalacji serwera zarządzającego;
- ✓ wymagania instalacji agentów aplikacji;
- ✓ zapewnienie komunikacji Klient-Serwer.

d). raportowanie – dobre praktyki i potrzeby wynikające z aktywności użytkowników;

e). możliwości kształtowania polityk – wariant per user, wariant per computer;

f). rozwiązywanie problemów;

g). weryfikacja poprawności działania środowiska;

h).podstawowe mechanizmy składowe – logi i zbieranie danych.

IV. <u>URZĄDZENIE DO KONTROLI DOSTĘPU DO SIECI LAN ZAMAWIAJĄCEGO</u> – 1 szt.

1. Urządzenie ma monitorować dostęp do sieci oparty na gotowych rozwiązaniach sprzętowych dostarczonych jako gotowe do użycia systemy ochrony. Rozwiązania mają także wykrywać luki systemowe i podatności serwerów, stacji roboczych i wszystkich urządzeń sieciowych, a także reagować na incydenty związane z malware i phishing. System musi oferować natychmiastowe powiadomienia, zbiorcze raporty, a także określać poziom ryzyka dla całej infrastruktury. **<u>Dostarczony system musi działać bezagentowo bez wykorzystania standardu 802.1x.</u>**

LP	Opis wymagań minimalnych
1.	Rozwiązanie na platformie sprzętowej dostarczone gotowe do użycia bez konieczności instalacji oprogramowania.
2.	Platforma sprzętowa musi posiadać co najmniej 2 interfejsy Gigabit w pełni konfigurowalne. System musi pozwalać na konfigurację pracy urządzenia w co najmniej 15 sieciach VLAN.
3.	System musi pracować w sieci co najmniej 85 hostów.
4.	Urządzenie musi zapewniać możliwość skanowania wszystkich urządzeń w infrastrukturze sieciowej. Licencja rozwiązania na posiadane moduły bezpieczeństwa i kontroli dostępu do sieci nie może być ograniczona.
5.	Produkt musi być autoryzowanym produktem korzystającym z bazy CVE (zarówno bazy głównej jak i bazy kandydatów) oraz bazy NVD (NationalVulnerability Database)
6.	Działanie badania podatności infrastruktury oparte na minimum trzech bazach w tym bazy CVE i NVD
7.	Możliwość wykrywania luk bezpieczeństwa w dowolnych systemach sieciowych bez instalowania dodatkowych aplikacji na tych systemach
8.	Możliwość weryfikacji bezpieczeństwa sieci w oparciu o normy bezpieczeństwa minimum: ISO27001/ISO17799, Sarbanes-Oxley, PCI-DSS.
9.	Rozwiązanie musi posiadać wbudowany system zarządzania zagrożeniami, przydzielania zleceń naprawy systemów wybranym pracownikom z możliwością nadzorowania postępu prac
10.	Urządzenie musi oferować szczegółowe raporty zawierające opisy wykrytych luk bezpieczeństwa wraz z informacją o możliwości ich wyeliminowania z danego systemu
11.	System musi posiadać wbudowany system raportowania z możliwością tworzenia podsumowań dla wskazanych systemów. system raportowania musi umożliwiać tworzenie raportów dla administratorów, a także ogólnych raportów podsumowujących poziom bezpieczeństwa. Raporty muszą być dostępne minimum w formatach PDF oraz xml.
12.	System musi posiadać mechanizm wykrywania aktywnego malware oraz aktywacji linków phishingowych przez użytkowników sieci. Na bazie zintegrowanych mechanizmów system musi blokować hosty zainfekowane malware lub aktywujące linki phishingowe.
13.	System musi umożliwiać wykrywanie i automatyczne blokowanie nieautoryzowanego dostępu do infrastruktury sieciowej w oparciu o zintegrowany, bezagentowy system Network Access Control.
14.	System musi umożliwiać wykrywanie i klasyfikowanie wszystkich urządzeń pracujących w infrastrukturze
15.	Rozwiązanie musi posiadać system wykrywania zmian w obrębie infrastruktury sieciowej i powiadamiania administratorów o każdej zanotowanej zmianie, powiadomienia nie mogą być wysyłane później niż 30 sekund po zanotowaniu zdarzenia
16.	System musi posiadać mechanizm automatycznego skanowania pod kątem występowania podatności i luk bezpieczeństwa zaufanych systemów podłączających się do infrastruktury sieciowej
17.	System musi wykrywać wszelkie anomalia sieciowe związane z MAC spoofing.
18.	Możliwość integracji ze smartswitchami (co najmniej HP, 3COM, CISCO, Extreme Networks, D-Link, Dell, Alcatel oraz Juniper)
19.	System musi umożliwiać automatyczne przełączanie hostów niezaufanych do nowopowstałego VLANu (tzw. Blackhole) lub do wskazanego przez administratora VLAN

	o niskim priorytecie dostępu.
20.	Rozwiązanie musi pozwalać na tworzenie użytkowników mających dostęp do interfejsu webowego na trzech różnych poziomach – managera, pracownika IT i operatora NAC.
21.	Możliwość wykrywania i powiadamiania o pojawieniu się w sieci hostów z danej puli adresów IP
22.	Możliwość monitorowania aktywności hostów i powiadamianie w przypadku braku łączności z monitorowanymi systemami/urządzeniami.
23.	Zarządzanie przez interfejs webowy, bez konieczności używania maszyny Javy ani dodatkowego oprogramowania instalowanego na maszynie zarządzającej.
24.	Praca urządzenia powinna być możliwa w sieciach z adresacją statyczną oraz w środowisku DHCP
25.	Urządzenie powinno umożliwiać określenie wykrytych luk bezpieczeństwa jako tzw. falsepositive dodatkowo powinna być możliwość generowania raportów podsumowujących, a także zbiorczych raportów dla osób zarządzających
26.	Minimum 3 tryby audytowe: pełny, porównawczy oraz inkrementalny
27.	Minimum roczna subskrypcja aktualizacji baz zagrożeń oraz firmware i roczne wsparcie techniczne producenta rozwiązania. W ramach maintenance także roczna gwarancja na urządzenie.

V. WDROŻENIE URZĄDZENIA DO KONTROLI DOSTĘPU DO SIECI LAN ZAMAWIAJĄCEGO.

1. Uruchomienie urządzenia i konfiguracja w siedzibie Zamawiającego. Konfiguracja będzie jednocześnie przedmiotem szkolenia wg nw. wymagań konfiguracja sieciowa rozwiązania.

1). Wdrożenie i szkolenie na miejscu w siedzibie Zamawiającego.

2). Omówienie najważniejszych elementów oferowanego rozwiązania przygotowanie do wdrożenia.

3). Konfiguracja sieciowa rozwiązania i wykorzystanie w infrastrukturze IT:

a). sieci fizyczne;

b). sieci VLAN;

c). integracja ze switchami zarządzalnymi;

d). segmentacja sieci a używanie NAC.

4). Omówienie podstawowych modułów NetShield:

a). Network Access Control;

b). Initial Scanning;

c). ADS – Asset Detection System – konfiguracja systemu;

d). Manage Assets – zarządzanie hostami, analiza zdarzeń.

5). Audyt.

a). konfiguracja audytów;

b). raporty i ogólne znaczenie zawartych informacji;

c). zarządzanie poaudytowe (workflow).

6). Malware Detection.

a). Jak analizować informacje zgromadzone przez Malware Detection

7).Logi i raporty.

8).Dashboard – jak rozumieć dane z Risk Profiler.

9). Najważniejsze dobre praktyki.

VI. <u>OPROGRAMOWANIE DO BACKUP-U:</u>

1. Oprogramowania do zabezpieczania danych poprzez mechanizm kopii zapasowych dedykowane dla środowisk wirtualizacyjnych – 2 szt.

Lp.	Wymagania minimalne
1.	1. Wspierane systemy operacyjne: 1). Dla hosta: • VMware ESX/ESX(i) 5.0, 5.1, 5.5, 6.0, 6.5 • Hyper-V 2). Dla maszyn wirtualnych • Windows 10,Windows 8/8.1/7/XP, Windows Vista; • Windows Server 2016,Windows Server 2012/2012R2, Windows Server 2008/2008R2; Windows Server 2003/2003R2; • Windows SBS 2011/2008, 2003/2003R2; • Windows Storage Server 2012/2012R2, 2008R2/2008/2003; • Windows MultiPoint Server 2012/2011/2010; • Linux OS (wiele dystrybucji); • macOS. 2. Wymagania związane z zarządzaniem systemem kopii zapasowych i wymagania co do oczekiwanych funkcjonalności: • interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www; • interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania system z poziomu tabletu); • zarządzanie procesem tworzenia kopii zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT; • definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem); • zdalna instalacja agentów kopii zapasowych na maszynach z systemem operacyjnym Windows; • zdalne uaktualniania agentów kopii zapasowych; • zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych. 3. Wymagane związane z wykonywaniem kopii zapasowych: • kopie zapasowe całych dysków i partycji; • kopie zapasowe wybranych plików i folderów; • technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWare ESXi); • kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory); • kopie zapasowe hostów Hyper-V i VMWare ESXi;

	• zapis kopii zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych; • zapis kopii zapasowych na udziały sieciowe; • zapis kopii zapasowych na serwer SFTP; • zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana; • wyszukiwanie plików w kopiach zapasowych; • szyfrowanie plików kopii zapasowych; • wsparcie dla technologii VSS; • kompresja plików kopii zapasowych; • replikacja kopii zapasowych na kolejny nośnik (dysk, magazyn chmurowy). 4. Wymagania związane z odtwarzaniem danych z kopii zapasowych: • odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore; • odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową; • odtworzenie całej maszyny wirtualnej; • odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej; • odtworzenie poszczególnych plików i folderów; • granularne odtwarzanie baz danych Microsoft Exchange; • granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange; • wyszukiwanie i podgląd odtwarzanych wiadomości email; • granularne odtwarzanie baz danych Microsoft SQL; • granularne odtwarzanie witryn i plików Microsoft SharePoint; • odtwarzanie kontrolerów domeny Microsoft Active Directory; • dla hostów VMware ESXi i Hyper-V – uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście. Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy. 5. Dodatkowe wymagania związane ochroną danych: • ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń • zapis kopii zapasowych na udziały sieciowe; • zapis kopii zapasowych na serwer SFTP; • zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana; • zapis kopii zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery); • możliwość wyszukiwania plików w kopiach zapasowych; • szyfrowanie plików kopii zapasowych; • wsparcie dla technologii VSS; • deduplikacja kopii zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć. • kompresja plików kopi zapasowych; • replikacja kopii zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy);

	• możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych 6. Wymagania związane z odtwarzaniem danych z kopii zapasowych: • odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore; • odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową; • odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej; • odtworzenie poszczególnych plików i folderów; • automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowaniu maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania); • granularne odtwarzanie baz danych Microsoft Exchange; • granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange; • wyszukiwanie i podgląd odtwarzanych wiadomości email; • granularne odtwarzanie baz danych Microsoft SQL; • granularne odtwarzanie witryn i plików Microsoft SharePoint; • odtwarzanie kontrolerów domeny Microsoft Active Directory; • granularne odtwarzanie baz danych Oracle; • Dla hostów VMware ESXi i Hyper-V – uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście. Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy. 7. Dodatkowe wymagania związane ochroną danych: • ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń. 8. Wymagania co do modelu licencjonowania rozwiązania: • możliwość wyboru przy zakupie licencji dożywotnich i subskrypcyjnych; • model licencjonowania oparty na maszynach fizycznych i hostach – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji).
2.	Wsparcie producenta oraz uprawnienia do aktualizacji - minimum 12 miesięcy.

2. Oprogramowania do zabezpieczania danych poprzez mechanizm kopii zapasowych dedykowane dla środowisk serwerowych – 1 szt.

Lp	Wymagania minimalne
1.	1. Wspierane systemy operacyjne: • Windows 10, Windows 8/8.1/7/XP, Windows Vista; • Windows Server 2016, Windows Server 2012/2012R2, Windows Server 2008/2008R2, Windows Server 2003/2003R2;

	• Windows SBS 2011/2008, 2003/2003R2; • Windows Storage Server 2012/2012R2, 2008R2/2008/2003; • Windows MultiPoint Server 2012/2011/2010; • Linux OS (wiele dystrybucji). 2. Wymagania związane z zarządzaniem systemem kopii zapasowych i wymagania co do oczekiwanych funkcjonalności: • interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www; • interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu tabletu); • zarządzanie procesem tworzenia kopii zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT; • definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem); • zdalna instalacja agentów kopii zapasowych na maszynach z systemem operacyjnym Windows; • zdalne uaktualniania agentów kopii zapasowych; • zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych. 3. Wymagane związane z wykonywaniem kopi zapasowych: • kopie zapasowe całych dysków i partycji; • kopie zapasowe wybranych plików i folderów; • kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory); • zapis kopii zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych; • zapis kopii zapasowych na udziały sieciowe; • zapis kopii zapasowych na serwer SFTP; • zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana; • wyszukiwanie plików w kopiach zapasowych; • szyfrowanie plików kopii zapasowych; • wsparcie dla technologii VSS; • kompresja plików kopii zapasowych; • replikacja kopii zapasowych na kolejny nośnik (dysk, magazyn chmurowy). 4. Wymagania związane z odtwarzaniem danych z kopii zapasowych: • odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore; • odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową; • odtworzenie całej maszyny wirtualnej; • odtworzenie poszczególnych plików i folderów; • granularne odtwarzanie baz danych Microsoft Exchange; • granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange;

	• wyszukiwanie i podgląd odtwarzanych wiadomości email; • granularne odtwarzanie baz danych Microsoft SQL; • granularne odtwarzanie witryn i plików Microsoft SharePoint; • odtwarzanie kontrolerów domeny Microsoft Active Directory. 5. Dodatkowe wymagania związane ochroną danych: • ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.
2.	Wsparcie Producenta oraz uprawnienia do aktualizacji - minimum 36 miesięcy.

VII. <u>LICENCJE DOSTĘPOWE SYSTEM SERWEROWY</u> - 60 SZT.

1. Wykonawca musi dostarczyć licencje dostępowe CAL na użytkownika do systemu serwerowego zgodnie z warunkami licencjonowania. Zamawiający użytkuje obecnie system Windows Serwer 2016.

VIII. <u>LICENCJE DOSTĘPOWE SYSTEM BAZODANOWY</u> - 20 SZT.

1. Licencja dostępowa CAL do SQL Server 2017 na użytkownika pozwalająca na dostęp do wersji : Enterprise Edition, Business Intelligence i Standard Edition.

IX. <u>BEZPRZEWODOWY PUNKT DOSTĘPOWY</u> - 3 SZT.

LP	Opis minimalnych parametrów
1.	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.
2.	Obudowa urządzenia musi być wykonana z tworzywa sztucznego i umożliwiać montaż na suficie wewnątrz budynku.
3.	Urządzenie musi być wyposażone w dwa niezależne moduły radiowe pracujące w pasmach i obsługiwać następujące standardy: 1. 2.4 GHz b/g/n 2. 5 GHz a/n/ac
4.	Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 14 SSID
5.	Liczba interfejsów Ethernet – 1 w standardzie 10/100/1000 Base-TX
6.	Interfejs radiowy urządzenia powinien wspierać następujące funkcje: MIMO – 2x2
7.	Maksymalna przepustowość interfejsu dla poszczególnych pasm: a) 2.4GHz – 300Mbps b) 5 GHz – 867 Mbps
8.	Wymagana moc nadawania min. 19dBm
9.	Wsparcie dla 802.11n 20/40Mhz HT
10.	Wsparcie dla kanału 80 MHz dla 802.11ac
11.	Anteny – 4 wbudowane, o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz
12.	Urządzenie musi być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz. Wymagane jest dostarczenie przez dostawcę odpowiednich urządzeń zasilających. W przypadku zasilania poprzez port ETH wymagane jest dostarczenie modułów typu „powerinjector”

	w standardzie 802.3at wraz z odpowiednim zasilaczem. W przypadku zasilania urządzenia przez zewnętrzny zasilacz wymagane jest dostarczenie odpowiedniego zasilacza.
13.	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

X. WDROŻENIE SYSTEMÓW.

LP	Obszar wdrożenia	Minimalne wymagania
1.	Serwery fizyczny zamawiającego	• Instalacja systemu operacyjnego wraz z wymaganymi aktualizacjami. • Uruchomienie środowiska wirtualnego Hyper-V4 maszyny wirtualne, z systemem wykorzystywanym przez Zamawiającego MS Windows Server 2016, zgodnie z wytycznymi Zamawiającego przedstawionymi na etapie instalacji i konfiguracji. • Instalacja i uruchomienie oprogramowania zarządzającego spełniającego minimalne wymagania dla dostarczonego z serwerem.
2.	Usługi - wdrożenie Active Directory	• Utworzenie struktury fizycznej AD; • Utworzenie struktury logicznej AD; • Konfiguracja usług powiązanych z AD; • Konfiguracja delegacji uprawnień AD; • Konfiguracja zabezpieczeń AD; • Konfiguracja użytkowników i komputerów w AD; • Konfiguracja stacji roboczych i wykonanie wdrożenia pilotażowego dla 70 komputerów ; • Dołączenie stacji roboczych do domeny wdrożenia pilotażowego dla 70 komputerów.
3.	System backup, serwery wirtualne i serwer fizyczny	• Musi być skonfigurowany zgodnie z wytycznymi administratora zamawiającego, w sposób umożliwiający na automatyczne tworzenie kopii bezpieczeństwa z systemów zainstalowanych na posiadanych serwerach Dell R730 – 4 instancje wirtualne Dell 530 – backup systemu MS Widnows Serwer 2012 R2 std; • Pomiędzy urządzeniami składającymi się na system backup-u muszą być wszystkie połączenia kablowe zapewniające poprawny przebieg procesu tworzenia kopii zapasowych; • Konfiguracja musi umożliwiać tworzenie kopii dziennych, tygodniowych, miesięcznych z możliwością zapisywania na zewnętrznym napędzie oraz odtwarzanie danych z wykonanych kopii zapasowych.