

Szczegółowy opis przedmiotu zamówienia, załącznik numer 1B do SIWZ

1. Wymagania techniczne dla rozwiązania chroniącego przed wyciekiem danych.

Zamawiający posiada obecnie funkcjonujący system typu Web Security firmy Websense (Web Security Suite) dla 400 Użytkowników. W ramach rozbudowy istniejącego funkcjonującego systemu, Zamawiający oczekuje dostarczenia licencji dla modułu ochrony przed wyciekiem danych (DLP - Data Lost Prevention) oraz ochrony ruchu internetowego użytkowników typu Web Security dla 500 użytkowników na okres 36 miesięcy wraz z wdrożeniem. Jednocześnie dostarczony moduł ochrony przed wyciekiem danych powinien spełniać następujące wymagania funkcjonalne:

1. Moduł musi zapewniać ochronę przed wyciekiem informacji zarówno w obszarze styku z Internetem (Network DLP) jak i na stacjach roboczych (Host DLP).
2. Moduł musi zostać dostarczony w postaci oprogramowania z dedykowanym centralnym systemem zarządzającym i raportującym. Centralny system zarządzania musi zapewniać możliwość zarządzania za pomocą jednej konsoli aplikacyjnej zarówno obecnie funkcjonującym modulem Web Security jak i dostarczonym modulem ochrony przed wyciekiem danych.
3. Moduł musi monitorować różne tryby pracy:
 - a. Monitorowanie danych podczas ich „przemieszczania się” (*Data in Motion*).
 - b. Monitorowanie danych podczas ich lokalnego wykorzystania np. kopiowanie na pamięć USB lub drukowania (*Data in Use*).
 - c. Pasywne odkrywanie położenia wrażliwych danych wewnątrz sieci korporacyjnej (*Data at Rest*).
4. Moduł powinien obsługiwać szeroki zakres kanałów komunikacyjnych (min.: Web, Email, Instant Messaging, drukowanie) i protokołów, bez względu na używany port.
5. Ochrona informacji powinna się opierać o reguły bezpieczeństwa odzwierciedlające procesy biznesowe.

6. Moduł powinien zapewnić pełne monitorowanie informacji w czasie rzeczywistym bez względu na miejsce ich występowania oraz sposób transmisji.
7. Moduł powinien dysponować pełnym raportowaniem użytkowników, grup i miejsc przechowywania danych.
8. Moduł powinien automatycznie kategoryzować/incydenty zdarzenia uwzględniając typ, regułę i poziom zagrożenia.
9. Wymagana jest automatyczna integracja z istniejącymi usługami katalogowymi Active Directory, aby umożliwić wyszukanie szczegółów aktywności użytkowników.
10. Moduł powinien dysponować predefiniowanymi regułami bezpieczeństwa (minimum 250 predefiniowanych reguł) niezależnie od możliwości definiowania własnych reguł i polityk.
11. W celu budowania reguł polityk konieczne jest automatycznie odkrywanie danych nieuporządkowanych jak i uporządkowanych (bazy danych) za pomocą bezagentowych narzędzi klasyfikujących, bez względu na typ lub format plików.
12. Moduł powinien mieć możliwość analizy chronionych informacji poprzez tworzenie wielokrotnego „odcisku palca” dla pojedynczego pliku poprzez jednokierunkową reprezentację matematyczną, analizując zawartość dokumentu.
13. Moduł powinien działać w oparciu o tzw. „świadomość kontekstową” - określenie jak informacją są i mogą być wykorzystywane, przez kogo oraz w jakim formacie i lokalizacji.
14. Tworzenie reguł bezpieczeństwa, automatyzacja procedur oraz zarządzanie incydentami musi odbywać się w czasie rzeczywistym.
15. Tworzenie raportów aktywności według lokalizacji, grupy lub użytkownika i analizowanie zachowania użytkowników
16. Moduł powinien być dostarczony z niezbędnymi licencjami wykorzystywanej bazy danych.

17. Moduł powinien zapewniać szyfrowanie repozytorium wewnętrznych kopii przechwyconych zdarzeń.
18. Moduł musi mieć możliwość analizowania całego ruchu sieciowego HTTP oraz HTTPS lokalnie na stacjach roboczych.
19. Moduł musi wspierać instalację agenta na co najmniej następujących systemach operacyjnych na stacjach roboczych: Windows XP(32-bit), Windows Vista (32-bit), Windows 7 (32-bit) oraz serwerach: Windows Server 2003 (32-bit) i Windows Server 2008 (32-bit).
20. Moduł powinien być dostarczony z licencjami zapewniającymi obsługę minimum 500 użytkowników oraz z subskrypcją i wsparciem technicznym producenta na okres 36 miesięcy dla systemu DLP oraz dla już posiadanego modułu Websense Web Security Suite. Wsparcie techniczne musi być dostępne 24 godziny na dobę, przez 7 dni w tygodniu i 365 dni w roku. W ramach wsparcia technicznego należy zapewnić dostęp do nowych wersji oprogramowania, sygnatur oraz bazy danych url. Wycena musi uwzględniać pełną instalację, uruchomienie i konfigurację niezbędnych modułów oprogramowania wraz z integracją z centralnym system zarządzającym. Zamawiający oprócz powyższego oczekuje także iż zaproponowane licencje rozszerzą funkcjonalność posiadanego systemu Websense TRITON o :
- Web Security Gateway
 - Email Security

Powyższe dwa moduły nie są przedmiotem wdrożenia aplikacji w tym postępowaniu.

2. Serwer typu RACK, konfiguracja 1- 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Maksymalnie 1U do instalacji w standardowej szafie RACK 19”, dostarczona wraz z szynami
Płyta główna	Płyta główna z możliwością zainstalowania minimum jednego procesora,

	również w technologii quad-core. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Procesor	Zainstalowany jeden procesor czterordzeniowy klasy x86, taktowany zegarem co najmniej 2,93GHz L3 8MB lub procesor równoważny wydajnościowo według wyniku testów przeprowadzonych przez Oferenta. W przypadku zaoferowania procesora równoważnego Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.
RAM	8GB DDR3 LV RDIMM 1333MHz, płyta główna powinna umożliwiać obsługę do 32GB pamięci RDIMM
Zabezpieczenia pamięci RAM	ECC, advanced ECC, SBEC, SDDC (lub równoważny)
Gniazda PCI	Minimum 2 złącza PCIe drugiej generacji w tym jedno PCIe x8, umożliwiające instalację kart pełnej wysokości.
Interfejsy sieciowe	Minimum 2 porty typu Gigabit Ethernet
Napęd optyczny	Wewnętrzny napęd DVD+/-RW
Dyski twarde	Możliwość instalacji minimum 4 dysków Hot-Plug 3,5": SATA, SAS. Zainstalowane 2 dyski 146GB typu Hot-Plug SAS 10 krpm
Kontroler RAID	Sprzętowy. Możliwość konfiguracji RAID: 0, 1, 5, 10, 6, 50, 60 z pamięcią cache minimum 512MB wyposażoną w podtrzymanie bateryjne.
Porty	6 x USB 2.0 z czego 2 na przednim panelu obudowy, 2 na tylnym panelu obudowy i dwa wewnętrzne, 2 x RJ-45, VGA
Video	Zintegrowana karta graficzna, umożliwiająca rozdzielczość min. 1280x1024.
Elementy redundantne HotPlug	Min. 2 Zasilacze
Zasilacze	Minimum 400W każdy
Bezpieczeństwo	Zintegrowany z płytą główną moduł TPM, możliwość zainstalowania wewnętrznej karty pamięci SD oraz klucza USB. Wbudowany czujnik otwarcia obudowy.
Karta Zarządzania	Możliwość instalacji karty zarządzającej niezależnej od zainstalowanego na serwerze systemu operacyjnego posiadającej dedykowane złącze RJ-45 i umożliwiającej: <ul style="list-style-type: none"> ▪ zdalny dostęp do graficznego interfejsu Web karty zarządzającej ▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera,) ▪ szyfrowane połączenie (SSLv3) oraz autentykację i autoryzację użytkownika ▪ możliwość podmontowania zdalnych wirtualnych napędów ▪ wirtualną konsolę z dostępem do myszy, klawiatury ▪ wsparcie dla IPv6 ▪ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, VLAN tagging, Telnet, SSH ▪ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer ▪ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny

	<ul style="list-style-type: none"> serwer ▪ integracja z Active Directory ▪ możliwość obsługi przez dwóch administratorów jednocześnie ▪ wsparcie dla dynamic DNS ▪ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej ▪ możliwość podłączenia lokalnego poprzez złącze RS-232
Oprogramowanie	Red Hat Enterprise Linux 6.0 wraz z 3 letnim wsparciem, Wymagany nośnik
Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001.</p> <p>Deklaracja CE.</p> <p>Wymagane jest dostarczenie odpowiednich certyfikatów.</p> <p>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla MS Windows Server 2008 w wersji x86, x64 i R2 x64.</p>
Warunki gwarancji	<p>Przynajmniej trzy lata gwarancji z czasem reakcji do 4 godzin od zgłoszenia.</p> <p>Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta serwera – dokumenty potwierdzające załączyć do oferty.</p> <p>Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.</p>
Dokumentacja użytkownika	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>

3. Serwer typu RACK, konfiguracja 2- 1 sztuka

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Maksymalnie 1U do instalacji w standardowej szafie RACK 19”, dostarczona wraz z szynami.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów, dwu lub czterordzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	<p>Dwa procesory czterordzeniowe klasy x86 dedykowane do pracy w serwerach zaprojektowane do pracy w układach dwuprocesorowych, taktowane zegarem co najmniej 2.13GHz, pamięć L3 8MB każdy lub procesor równoważny wydajnościowo według wyniku testów przeprowadzonych przez Oferenta.</p> <p>W przypadku zaoferowania procesora równoważnego Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów</p>

	wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.
RAM	8GB RDIMM DDR3, płyta musi umożliwiać obsługę do minimum 64GB, na płycie głównej powinno znajdować się minimum 8 slotów przeznaczonych dla pamięci.
Zabezpieczenia pamięci RAM	ECC, Memory Mirror
Gniazda PCI	Minimum 1 złącza PCIe x16.
Interfejsy sieciowe	Minimum 2 złącza typu 10/100/1000 wbudowane na płycie głównej. Dodatkowa dwuportowa karta sieciowa Gigabit Ethernet z wsparciem dla TOE.
Napęd optyczny	Wewnętrzny napęd DVD+/-RW
Dyski twarde	Możliwość instalacji dysków SATA, SAS. Zainstalowane 2 dyski 300GB typu HotPlug SAS 3,5" 15krpm skonfigurowane w RAID1. Możliwość instalacji dodatkowych 2 dysków twardych Hot-Plug.
Kontroler RAID	Dedykowany, umożliwiający konfigurację RAID: 0, 1.
Porty	6 x USB 2.0 z czego 2 na przednim panelu obudowy, 2 na tylnym panelu obudowy i dwa wewnętrzne, 2 x RJ-45, VGA
Video	Zintegrowana karta graficzna, umożliwiająca rozdzielczość min. 1280x1024.
Elementy redundantne HotPlug	Min. 2 Zasilacze
Zasilacze	Redundantne, Hot-Plug o mocy maksymalnie 500W każdy.
Bezpieczeństwo	Zintegrowany z płytą główną moduł TPM, możliwość zainstalowania wewnętrznej karty pamięci SD lub klucza USB.
Diagnostyka	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	<p>Możliwość instalacji karty zarządzającej niezależnej od zainstalowanego na serwerze systemu operacyjnego posiadającej dedykowane złącze RJ-45 i umożliwiająca na:</p> <ul style="list-style-type: none"> ▪ zdalny dostęp do graficznego interfejsu Web karty zarządzającej ▪ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera,) ▪ szyfrowane połączenie (SSLv3) oraz autentykację i autoryzację użytkownika ▪ możliwość podmontowania zdalnych wirtualnych napędów ▪ wirtualną konsolę z dostępem do myszy, klawiatury ▪ wsparcie dla IPv6 ▪ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, VLAN tagging, Telnet, SSH ▪ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer ▪ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer ▪ integracja z Active Directory ▪ możliwość obsługi przez dwóch administratorów jednocześnie ▪ wsparcie dla dynamic DNS ▪ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej

	<ul style="list-style-type: none"> możliwość podłączenia lokalnego poprzez złącze RS-232
Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001.</p> <p>Deklaracja CE.</p> <p>Wymagane jest dostarczenie odpowiednich certyfikatów.</p>
System Operacyjny	Red Hat Enterprise Linux 6.0 wraz z 3 letnim wsparciem, wymagany nośnik
Warunki gwarancji	<p>Przynajmniej trzy lata gwarancji z czasem reakcji do czterech godzin od zgłoszenia.</p> <p>Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty.</p> <p>Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.</p> <p>Zamawiający oczekuje możliwości przedłużenia czasu gwarancji do pięciu lat.</p>
Dokumentacja użytkownika	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>