Załącznik Nr 6-2 do SWZ

Szczegółowy opis przedmiotu zamówienia

Zadanie nr 2 - Dostawa oprogramowania

2.1. Dostawa oprogramowania do backupu

Przedmiot zamówienia obejmuje dostawę licencji na oprogramowanie do zabezpieczenia środowiska obejmującego serwery zwirtualizowane. Licencje muszą umożliwić zabezpieczenie (backup i odtwarzania) 2 maszyn wirtualnych pracujących w środowisku liczącym 2 fizyczne procesory.

Oprogramowanie musi wspierać (wymagane jest wsparcie producenta) minimum następujące systemy operacyjne: Microsoft Windows, Backup zasobów plików w przypadku powyższych systemów musi podlegać de-duplikacji.

Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych i aplikacji: MS SQL, Oracle, Hyper-V. Backup powyższych baz danych i aplikacji musi podlegać de-duplikacji.

Oprogramowanie backupowe musi umożliwiać dla sieci lokalnej:

- backup pojedynczych plików,
- backup całych systemów plików,
- backup baz danych w trakcie ich normalnej pracy,
- backup ustawień systemu operacyjnego Windows,
- backup całych obrazów maszyn wirtualnych systemu Hyper-V.

Oferowane rozwiązanie backupowe musi umożliwiać odtworzenie:

- plików, baz danych, na docelową maszynę - z poziomu centralnej konsoli systemu backupowego;
- wymagany scenariusz nie może wymagać logowania się na odtwarzaną maszynę w celu odtworzenia danych z systemu backupowego.

Wymagana jest możliwość definiowania w konsoli oprogramowania backupowego ważności (retencji) danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte.

Wymagana jest możliwość tworzenia z poziomu GUI (konsoli graficznej), polityk w których zdefiniowano:

- okres przechowywania backupów dziennych,
- okres przechowywania backupów tygodniowych,
- okres przechowywania backupów miesięcznych,
- okres przechowywania backupów rocznych.

Konsola zarządzająca systemem backupowym powinna integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról (min, administrator, monitoring, tylko odtwarzanie danych) w systemie backupowym.

Wymagana jest możliwość generowania (poprzez konsolę) raportów określających zajętość przestrzeni przeznaczonej na składowanie de-duplikatów.

Bloki przesyłane z zabezpieczanych serwerów do oferowanych deduplikatorów muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256- bitowym.

Oferowany system musi pozwalać na:

- odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej, funkcjonalność ta musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows, możliwość zamontowania na dowolnym serwerze (fizycznym lub wirtualnym) zbackupowanych obrazów maszyn wirtualnych Windows (plików vmdk maszyny wirtualnej Windows), w efekcie metoda ta nie odtwarza backupów a jedynie umożliwia na przeglądanie zawartości plików vmdk w backupie z poziomu Eksploratora Plików Windows na dowolnej maszynie. Powyższe metody odtworzenia muszą być wbudowane w system backupu i w pełni automatyczne nie mogą generować konieczności wykorzystania dodatkowych skryptów/ komend.
- na szybkie odtworzenie: całych obrazów maszyn wirtualnych, pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej.

Wymaga się aby oferowany system backupu posiadał możliwość bezpośredniego raportowania o błędach do serwisu producenta.

W ramach dostarczonych licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania z użycia komponentów systemu backupowego oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego. Wymagana dostępność następujących raportów:

- podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych),
- podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych danych),
- zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów,
- zbiorcze zestawienie zabezpieczanych serwerów które w sposób ciągły (kilka razy pod rząd) maja problem z backupami,
- zestawienie zabezpieczanych systemów plików, które nie są backupowane,
- spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii),
- najmniej wiarygodne zabezpieczanych serwery (procent nieudanych backupów),
- lista najwolniejszych/najszybszych zabezpieczanych maszyn,
- liczba danych backupowanych,
- liczba zadań backupowych,
- zużycie zasobów na serwerach backupowych (procesor, pamięć, karty sieciowe LAN),
- zużycie mediów backupowych,
- aktualna konfiguracja systemu backupowego,

- historia zmian konfiguracji systemu backupowego.

W ramach dostarczonych licencji musi istnieć możliwość zaindeksowania oraz przeszukiwania backupów z poziomu graficznego interface'u (GUI), wymagana także możliwość wyszukania dowolnych fraz w nazwach plików.

Oprogramowanie musi posiadać możliwość trybu pracy umożliwiającego objęciem protekcją w sposób automatyczny nowo dodanych maszyn wirtualnych (VM).

Oprogramowani musi posiadać wsparcie dla VSS, zapewnienie konsystencji aplikacji na poziomie VSS.

Wymagane jest dostarczenie licencji zapewniających funkcjonalność: ENCRYPTION (szyfrowanie) w obrębie maksymalnej wymaganej pojemności urządzenia.

Musi istnieć możliwość uruchomienia zdalnych konsol dla:

- aplikacji backup'owej,
- systemu dedykowanego do raportowania,
- systemu dedykowanego do przeszukiwania danych backup'owych.

Zapewnienie podglądu on-line takich elementów jak:

- aktywność procesów backup'owych,
- aktywność procesów replikacyjnych,
- aktualny status,
- alarmy w przypadku zaoferowanej aplikacji backup'owej oraz deduplikatora.

Możliwość zarządzania procesem wyszukiwania danych backup'owych.

Integracja z oferowanym rozwiązaniem dedykowanym do raportowania, możliwość inicjowania raportów.

2.2. Dostawa oprogramowania AV z zaawansowanymi funkcjami

Przedmiot zamówienia obejmuje dostawę 45 szt. licencji na oprogramowanie antywirusowe z zaawansowanymi funkcjami na okres 24 miesięcy.

- Zamawiający informuje, iż obecnie korzysta z oprogramowania antywirusowego Bitdefender GravityZone Business Security wraz z dodatkiem GravityZone Patch Management i oprogramowanie to jako oprogramowanie referencyjne spełnia jego wymogi jakościowe i funkcjonalne. W przypadku dostarczenia tego oprogramowania wystarczające jest dostawa wyłącznie licencji i kluczy licencji.
- Zamawiający dopuszcza jednak dostarczenie innego równoważnego oprogramowania do oprogramowania antywirusowego Bitdefender GravityZone Business Security wraz z dodatkiem GravityZone Patch Management pod warunkiem:
- Dostarczenia nowych licencji nowego oprogramowania zgodnie z ilościami, oraz okresami podanymi wyżej.
- Dostarczenie instrukcji instalacji i konfigurowania oprogramowania.

- Nowe oprogramowanie antywirusowe musi być kompatybilne z systemami rodziny Microsoft Windows Server 2016, 2019, 2022, Microsoft Windows 7, 8.1, 10, 11, Apple Mac OS, oraz na urządzeniach mobilnych z systemem Android, Apple iOS.
- Przeszkolenia administratora najpóźniej w dniu dostarczenia kluczy licencyjnych. Zakres szkolenia dotyczy administrowania od strony konsoli zarządzającej oprogramowaniem, konfigurowanie i administrowanie od strony klienta. Szkolenie odbędzie się w siedzibie Zamawiającego.
- Równoważny system antywirusowy musi spełniać również następujące wymagania:
    - Program posiada zintegrowaną i scentralizowaną konsola chmurową, która zapewnia zarządzanie z poziomu jednej konsoli dla wszystkich komponentów bezpieczeństwa.
    - Patch Management – zarządzanie procesem aktualizowania stacji roboczych tj. aktualizacje Windows Update oraz oprogramowania firm trzecich. Patch Management ma umożliwiać zautomatyzowaną aktualizacje oprogramowania poprzez konfigurowalne zadanie wykonywane z serwera zarządzającego oprogramowaniem antywirusowym z możliwością zablokowania, wycofania lub deinstalacji nie chcianych bądź wadliwych aktualizacji na wszystkie lub wybrane stacje robocze/serwery. Funkcjonalność testowej instalacji aktualizacji na wybranej grupie stacji roboczych.
    - Disk Encryption - Pełne szyfrowanie dysku wykorzystuje mechanizmy szyfrowania urządzeń, dostarczane przez system Windows (BitLocker) i Mac (FileVault), w celu zapewnienia zgodności i wydajności. Jest w pełni zintegrowany z konsolą GravityZone i agentem, co umożliwia szybkie i bezproblemowe wdrażanie szyfrowania dysków.
    - Możliwość skanowania komputerów offline tj. poza godzinami pracy. Oprogramowanie antywirusowe (serwer administracyjny) ma umożliwiać utworzenie zadania uruchomienia wyłączonych komputerów po godzinach pracy (ustawione zadanie wg. Terminarza).
    - Blokowanie dostępu dysków USB – kontrola urządzeń (pendrive, dyski zewnętrzne inne nośniki pamięci).
    - Możliwość skonfigurowania przez administratorów dostępu dla firmowych dysków USB (pendrive, dyski zewnętrzne inne nośniki pamięci).
    - Zadanie automatycznego skanowania zawartości zezwolonych dysków USB, które podłączane są do stacji roboczych.
    - Możliwość automatycznej (zdalnej) instalacji oprogramowania antywirusowego na stacjach klienckich, bez dostępu do Internetu.
    - Umożliwienie automatycznej aktualizacji i dystrybucji baz sygnatur wirusów i aktualizacji programu w sieci wydzielonej, bez dostępu do Internetu.
    - Umożliwienie zdalnej instalacji oprogramowania firm trzecich na stacje robocze z poziomu serwera administracyjnego (tworzenia paczek instalacyjnych).
    - Statystyki ochrony w czasie rzeczywistym, bieżące stany urządzeń, raport zagrożeń, raport infekcji chronionych urządzeń, raport o aktualnych wersjach programu antywirusowego, wersji agenta, definicji baz wirusów. Raporty o przebiegu aktualizacji oprogramowania (patch management) Windows Update oraz oprogramowania firm trzecich.

- Automatyczne powiadamianie administratorów (drogą mailową) o wykrytym zagrożeniu w czasie rzeczywistym. Użytkownicy mają widzieć powiadomienia w interfejsie aplikacji, zdefiniowane przez administratorów.
- Możliwość wykrywania i usuwania innego oprogramowania antywirusowego podczas instalacji.
- Możliwość zablokowania/ukrycia interfejsu przed użytkownikiem, zezwolenie na dostęp tylko do wybranych funkcji/zadań zezwolonych przez administratorów. Deinstalacja lub wyłączenie oprogramowania antywirusowego zabezpieczone przed użytkownikiem poprzez login oraz hasło administracyjne.
- Możliwość instalacji konsoli administracyjnej na kilku wybranych stanowiskach. Konsola zarządzająca oraz serwer administracyjny mają zapewniać automatyczną synchronizację z Active Directory.
- Program ma posiadać kwarantannę z której można przywrócić lub trwale usunąć zainfekowane piki.
- Program ma posiadać kontrolę aplikacji oraz możliwość definiowania białych i czarnych list uruchamianego oprogramowania. Możliwość blokowania komunikatorów sieciowych (audio–video), zezwalanie bądź blokowanie zintegrowanych lub zewnętrznych kamer video (zarządzanie urządzeniami).
- Ochrona przed exploitami , heurystyka.
- Ochrona sieci, zdefiniowanie zaufanych sieci. Niezależny od systemowego firewall. Automatyczna dezaktywacja zapory systemu Windows na czas działania oprogramowania antywirusowego. Możliwość blokowania komputera z którego przeprowadzane jest skanowanie portów na określony czas poprzez automatyczne blokowanie na firewallu.
- MDM – Mobile Device Management – moduł do zarządzania i instalowania oprogramowania antywirusowego.

2.3. Dostawa oprogramowania do inwentaryzacji i oprogramowania

Dostawa i wdrożenie informatycznego systemu zarządzania zasobami i użytkownikami, na który składają się monitoring infrastruktury, inwentaryzacja, monitoring pracy, helpdesk, ochrona danych przed wyciekiem.

Wymagania względem licencji:

Dostarczone licencje na oprogramowanie muszą być bezterminowe.

Dostarczone licencje oprogramowanie muszą być dostarczone z 12 miesięcznym wsparciem producenta, liczonym od daty zakończenia wdrożenia. W ramach wsparcia wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.

Dostarczone licencje na oprogramowanie muszą objąć co najmniej 50 stanowisk roboczych i nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów, jak drukarki, monitory czy urządzenia sieciowe.

Podstawowe informacje techniczne o Przedmiocie Zamówienia:

1. System musi posiadać budowę modułową i składać się z serwera zarządzającego, zdalnych konsoli oraz agentów.

2. Komunikacja pomiędzy składnikami systemu musi być nawiązywana przy użyciu szyfrowanego protokołu.

3. Baza danych musi być oparta na darmowym silniku SQL.

4. Dane z monitoringu działań pracownika na stanowisku roboczym muszą być odseparowane od informacji o stacji roboczej. Musi być zachowana zgodność z RODO, która umożliwia usunięcie danych o pracowniku bez konieczności usuwania danych stacji roboczej.

5. Program musi posiadać ochronę (hasło Głównego Administratora) przed usunięciem lub ingerencją użytkownika (nawet z prawami administracyjnymi na stacji roboczej).

6. System musi być dostępny w polskiej i angielskiej wersji językowej.

Poniżej zawarty został opis funkcjonalności poszczególnych modułów systemu.

1. Monitorowanie infrastruktury. System musi spełniać wymagania, takiej jak:

- Wykrywanie urządzeń wpiętych w sieć wewnętrzną poprzez skanowanie ping oraz argping (bezagentowe).
- Wizualizacja graficzna stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci.
- Wizualizacja połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie.
- Wykrywanie serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program musi monitorować czas odpowiedzi serwisów i procent utraconych pakietów.
- W przypadku serwerów pocztowych: 2 program musi monitorować zarówno serwis odbierający, jak i wysyłający pocztę.
- program musi mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS).
- program musi mieć możliwość wykonywania operacji testowych, program musi mieć możliwość wysyłania powiadomień, w przypadku gdy serwer pocztowy nie odpowiada.
- System musi umożliwiać monitorowanie serwerów WWW i adresów URL.
- System musi obsługiwać szyfrowanie SSL/TLS w powiadomieniach e-mail.
- System musi obsługiwać urządzenia SNMP wspierające SNMP v1/2/3 z szyfrowaniem.
- System musi obsługiwać komunikaty syslog i pułapki SNMP.
- System musi umożliwiać monitoring routerów i przełączników według:

- zmian stanu interfejsów sieciowych,
- ruchu sieciowego,
- podłączonych stacji roboczych (w tym graficzna prezentacja panelu switcha),
- ruchu generowanego przez podłączone do portów stacje robocze.

- Monitorowanie serwisów Windows – oprogramowanie musi alarmować gdy serwis przestanie działać oraz musi umożliwiać jego uruchomienie, zatrzymanie i zrestartowanie.
- Monitorowanie wydajności systemów Windows.
- Oprogramowanie musi posiadać funkcję kompilatora plików MIB.
- System musi umożliwiać tworzenie graficznych map zarządzania logiczną strukturą urządzeń.

2. Inwentaryzacja. W zakresie inwentaryzacji system musi umożliwiać:

- Automatyczne gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych.
- Automatycznie generowanie:
  - zestawienia posiadanych konfiguracji sprzętowych,
  - wolnym miejscu na dyskach,
  - średniego wykorzystania pamięci,
  - informacje o koniecznym upgrade.
- System musi wyświetlać informacje o zainstalowanych aplikacjach oraz aktualizacjach Windows.
- System musi zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej, tj. instalacji i deinstalacji aplikacji, zmian adresu IP itd.
- Wysyłanie powiadomień w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
- System musi umożliwiać odczytanie numeru seryjnego (kluczy licencyjnych).
- System musi umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
- System musi umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
- System musi umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem znalezionych na stacjach roboczych oraz ich zdalne usuwanie.
- System musi mieć możliwość wymiany plików do i ze stacją roboczą poprzez funkcję menadżera plików. Działania Administratorów wykonywane w tej funkcji muszą być logowane.

3. W zakresie prowadzenia baz ewidencji majątku IT:

- System musi umożliwiać przechowywanie wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji.
- Wymagana jest możliwość definiowania własnych typów wyposażenia, ich atrybutów oraz wartości oraz możliwość importu danych z zewnętrznego źródła (np. CSV).
- Generowanie zestawień wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania.
- Archiwizacja i porównywanie audytów środków trwałych.
- Tworzenie kodów kresowych w środkach trwałych.
- Drukowanie kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy.
- Inwentaryzacja sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej (należy wskazać dedykowany system dla aplikacji).
- System musi móc przeprowadzać inwentaryzację stacji roboczych niepodłączonych do sieci.
- Możliwość definiowania alarmów z powiadomieniami e-mail dla dowolnych pól typu data ze szczegółów środków trwałych lub licencji (np. powiadomienie o wygasającej licencja/gwarancja).
- Agenty inwentaryzacji muszą być dostępne dla systemów Android, macOS oraz Linux.
- Funkcje inwentaryzacji oprogramowania muszą umożliwiać:
    - Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
    - Zarządzanie posiadanymi licencjami.
    - Audyt legalności oprogramowania oraz powiadamiania w przypadku przekroczenia liczby posiadanych licencji.
    - Tworzenie raportów zgodności licencji.
    - Przypisanie do programów numerów seryjnych lub wartości.
    - Monitorowanie aktywności pracowników oraz zarządzanie czasem pracy poprzez: Faktyczny czas aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy).
    - Monitorowanie procesów wraz z informacją o uruchomieniu na podwyższonych uprawnieniach.
    - System musi obrazować rzeczywiste użytkowanie programów (procentowa wartość wykorzystania aplikacji), czas używania aplikacji w stosunku do łącznego czasu, przez który aplikacja była uruchomiona (informacja, na którym komputerze wykonano daną aktywność).
    - System musi monitorować ruch lokalny i transfer internetowy generowany przez użytkowników.
    - Oprogramowanie musi monitorować wydruki.

- Oprogramowanie musi monitorować nagłówki przesłanej przez użytkownika poczty email.

Dodatkowo system musi umożliwiać:

• Blokowanie ruchu na wskazanych portach TCP/IP.

• Blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem.

• Wysyłanie powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny,

• Przygotowanie metryki ustawień monitorowania użytkownika w postaci raportu.

• Generowanie raportów dla użytkowników Active Directory.

• Blokowanie uruchamiania aplikacji.

4. Zarządzanie czasem i analiza aktywności użytkowników musi tworzyć:

• Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.

• Statystyki aktywności podwładnych widoczne dla przełożonego.

• Listę odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.

• Statystyki popularności stron internetowych i aplikacji w organizacji, grupie i u poszczególnych użytkowników.

W zakresie zdalnej pomocy i bazy wiedzy system musi posiadać następujące funkcjonalności:

- Kontrolę stacji użytkownika poprzez podgląd pulpitu użytkownika z możliwością przejęcia nad nim kontroli (zarówno użytkownik jak i administrator muszą widzieć ten sam ekran).
- Administrator w trakcie zdalnego dostępu musi mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika.
- System musi umożliwiać monitorowanie przez użytkowników procesu rozwiązywania zgłoszonych przez nich problemów i aktualnych statusów, jak również musi mieć możliwość wymiany informacji z Administratorem poprzez komentarze, które muszą być wpisywane i widoczne dla obu stron.
- Oprogramowanie może posiadać wbudowany komunikator, który musi umożliwiać przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami.
- System musi posiadać możliwość tworzenia i rozwijania bazy wiedzy pomagającej użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy.
- System musi umożliwiać pobieranie listy użytkowników z Active Directory.
- System musi umożliwiać Administratorom tworzenie drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii (maksymalnie do 4 poziomów kategorii).
- System musi umożliwiać przypisywanie poszczególnych Administratorów do kategorii zgłoszeń.
- System musi umożliwiać procesowanie zgłoszeń użytkowników z wiadomości e-mail.

- Tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń.
- Oprogramowanie musi umożliwiać dołączanie załączników do zgłoszeń.
- System musi umożliwiać tworzenie i dodawanie do zgłoszenia zrzutów ekranowych.
- System musi umożliwiać dystrybucje oprogramowania oraz uruchamianie plików za pomocą dedykowanych agentów (w tym plików z rozszerzeniem MSI).
- System musi umożliwiać kolejkowanie dystrybucji plików, w przypadku gdy w trakcie trwania operacji stacja robocza jest wyłączona.
- Program musi umożliwiać zdalne wykonywanie poleceń poprzez agentów na stacjach roboczych.
- System musi umożliwiać zarządzanie procesami systemu Windows w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami.
- System musi umożliwiać wymianę plików do i ze stacji roboczej poprzez wbudowaną funkcję menedżera plików.