DZ-751-83/25

*[nazwa Wykonawcy] Załącznik 23.3.3.*

**Pakiet nr 3**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Oprogramowanie do monitorowania pracy komputerów** | | | | | | | | | |
| Lp. | Nazwa | Ilość | Cena jedn. netto | Wartość netto | | Stawka VAT w % | | Wartość brutto | |
| 1. | **Oprogramowanie do monitorowania pracy komputerów** | 1 kpl. |  |  | |  | |  | |
| RAZEM | | | | |  | |  | |  |

**ZESTAWIENIE WYMAGANYCH – OFEROWANYCH**

**PARAMETRÓW TECHNICZNYCH I UŻYTKOWYCH**

|  |  |  |
| --- | --- | --- |
| 1. | **Oprogramowanie do monitorowania pracy komputerów** | |
| Nazwa |  |
| Producent/kraj |  |
| Typ/Model |  |
| Rok produkcji |  |
| **Lp.** | **Parametr nie gorszy niż/ warunek wymagany** | **Parametr oferowany – podać** |
| **I Ogólne** | | |
| 1 | Fabrycznie nowe, rok produkcji nie starszy niż 2025 |  |
| 2 | Instrukcja obsługi w języku polskim w wersji papierowej, karta gwarancyjna dostarczone wraz z urządzeniem. |  |
| 3 | Szkolenie personelu |  |
| 4 | Dostawa, montaż i uruchomienie w miejscu wskazanym przez Zamawiającego |  |
| **II Opis** | |  |
| 1 | System monitorowania aktywności użytkowników oraz komputerów musi posiadać budowę modułową, czyli serwera zarządzającego, zdalnych konsoli oraz agentów wdrażanych na komputerach użytkowników. Moduły muszą umożliwiać monitoring aktywności użytkowników oraz sprzętu komputerowego pod kątem zmian sprzętowych i programowych.  . |  |
| 2 | System musi pozwalać na tworzenie dowolnej liczby administratorów oraz integrację z Active Directory po protokole LDAPS. |  |
| 3 | System powinien zawierać możliwość uruchomienia usługi weryfikacji dwuskładnikowej (MFA) dla kont administratorów |  |
| 4 | System musi posiadać system raportowania. Musi posiadać predefiniowane raporty oraz powinien pozwalać na tworzenie własnych zestawień. |  |
| * 1. **Monitorowanie aktywności użytkowników** | |  |
| 5 | System musi zbierać następujące dane o aktywności użytkowników:  1. Faktyczny czas aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy).  2. Informacje dotyczące używanych procesów wraz z informacją o uruchomieniu na podwyższonych uprawnieniach.  3. Rzeczywisty czasu użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazującą czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność.  4. Informacje o edytowanych przez użytkownika plikach.  5. Lista odwiedzanych stron WWW (tytuły, adresy, kategorie, liczba i czas wizyt).  6. Transfer sieciowy użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika).  7. Wydruki m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika, zestawienia pod względem stacji roboczej.  8. Nagłówki przesyłane w aplikacjach klienckich poczty e-mail. |  |
| 6 | Powinna istnieć także możliwość uruchomienia wykonywania cyklicznych zrzutów ekranowych dla określonej grupy komputerów użytkowników |  |
| 7 | System powinien także wykrywać podejrzaną aktywność, która ma na celu symulacje faktycznej pracy. |  |
| 8 | System powinien umożliwiać blokowanie stron internetowych poprzez zezwolenie lub zablokowanie całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen. |  |
| 9 | System musi mieć możliwość przygotowywania zestawienia aktywności użytkowników w formie raportów. |  |
| 10 | System powinien mieć możliwość blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzenie przez użytkowników. |  |
| * 1. **Ochrona danych przed wyciekiem** | |  |
| 11 | W ramach ochrony danych przed wyciekiem systemu musi posiadać następujące funkcjonalności:  1. Blokowanie urządzeń i nośników danych.  2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.  3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.  4. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.  5. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.  6. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.  7. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.  8. Tworzenie list (map) komputerów, które zostały już zaszyfrowane, lub jeszcze nie zostały zaszyfrowane.  9. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.  10. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.  11. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.  12. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM. |  |
| 12 | Ponadto system musi umożliwiać zarządzanie prawami dostępu do urządzeń, tj.:  1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.  2. Autoryzowanie urządzeń służbowych (przykładowo szyfrowanych): pendrive’ów, dysków itp.  3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.  4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.  5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane. |  |
| 13 | System musi prowadzić także audyt operacji na urządzeniach przenośnych i komputerach w zakresie modyfikacji plików:  1. Zapisywać informacje o zmianach w systemie plików.  2. Każdorazowe podłączenie/odłączenie urządzenia przenośnego powinno być odnotowane w systemie.  3. Każdorazowe naruszenie blokad powinno być rejestrowane. |  |
| * 1. **Inwentaryzacja sprzętu i oprogramowania** | |  |
| 14 | System powinien gromadzić następujące informacje o sprzęcie oraz oprogramowaniu użytkowników:  1. Szczegóły dotyczące: modelu komputera, procesora, pamięci, płyty głównej, napędów, kart, podłączonych urządzeń.  2. Szczegółowe dane o pracy dysków.  3. Konfigurację sprzętową, wolne miejsce na dyskach, średnie wykorzystanie pamięci.  4. Zainstalowane aplikacje oraz aktualizacje systemu Windows.  5. Zmiany przeprowadzone na stacji roboczej, tj. instalacje/deinstalacje aplikacji, zmiany adresu IP itd. |  |
| 15 | System powinien móc umożliwiać następujące czynności w zakresie inwentaryzacji:  1. Odczytanie numerów seryjnych (kluczy licencyjnych).  2. Automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacyjnych wymaganych oraz nieautoryzowanych.  3. Przegląd informacji o konfiguracji systemu: komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań.  4. Utworzenie listy plików użytkowników z określonych rozszerzeniem znalezionych na stacjach roboczych oraz ich zdalne usuwanie.  5. Wymianę plików do i ze stacją roboczą.  6. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.  7. Gromadzenie informacji o aplikacjach używanych w organizacji.  8. Tworzenie własnych wzorców aplikacji.  9. Zarządzanie posiadanymi licencjami.  10. Wskazywanie osób odpowiedzialnych za licencję.  11. Wskazanie użytkowników licencji. |  |
| * 1. **Pomoc zdalna użytkownikom** | |  |
| 16 | System powinien umożliwiać zdalny podgląd pulpitu użytkownika i przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połączenie i opcją odrzucenia takiego połączenia przez użytkownika |  |
| 17 | Dodatkowo musi istnieć możliwość zasłonienia ekranu przed użytkownikiem, aby nie widział czynności wykonywanych przez administratora. |  |
| 18 | Administrator w trakcie zdalnego dostępu musi mieć możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. |  |
| * 1. **Ochrona przed usunięciem** | |  |
| 19 | Agent instalowany na komputerze użytkownika musi mieć wbudowane zabezpieczenia chroniące przed jego wyłączeniem czy też usunięciem przez osoby do tego nieuprawnione |  |

1. **Wymagania**

W ramach wdrożenia Zamawiający oczekuje:

* 1. Konfiguracji serwerów/urządzeń na lokalnym środowisku wirtualnym Zamawiającego. W przypadku konieczności instalacji systemu na serwerze fizycznym – Wykonawca musi ten serwer zapewnić.
  2. Instalacji oraz konfiguracji oprogramowania.
  3. Testów rozwiązania.
  4. Instruktażu dla administratorów demonstrujący sposób zarządzania środowiskiem.
  5. Dostarczenia dokumentacji powdrożeniowej składającą się z następujących elementów:
* Zakresu wykonanych czynności oraz uruchomionych funkcjonalności.
* Końcowych nazw oraz szczegółowej adresacji poszczególnych elementów.
* Komplety poświadczeń do całej infrastruktury – wymagana zmiana haseł domyślnych dostarczone jako osobny załącznik w postaci zaszyfrowanego pliku kdbx,.
  1. Po zakończonym wdrożeniu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników”.

1. **Pozostałe wymagania:**
   1. Zamawiający wymaga aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:
      1. posiadane środowisko domenowe,
      2. posiadaną konfigurację sieci wraz z segmentacją VLAN, oraz strefą DMZ,
      3. posiadaną konfiguracją baz danych i backupów,
      4. konfigurację stacji roboczych.
   2. Zamawiający wymaga by osoby administrujące systemami monitorowania pracy użytkowników i komputerów posiadały odpowiednie kompetencje potwierdzone odbytym szkoleniem.
   3. Całość dostarczanego oprogramowania standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
   4. Całość dostarczanego rozwiązania, musi być nowe, wcześniej nieużywane, rok produkcji nie starszy niż 2025.
   5. Całość dostarczanego rozwiązania, w którym nie wskazano szczegółowych warunków gwarancji, musi być objęte minimum 36 miesięczną gwarancją obejmującą trwałość projektu , której start biegnie od dnia podpisania protokołu odbioru
   6. System i jego komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
   7. Do systemu musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
   8. Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji.
   9. Wykonawca na czas instalacji otrzyma dostęp VPN do serwera, na którym system zostanie wdrożony. Czynności serwisowe, gwarancyjne po okresie wdrożenia będą odbywały się poprzez zestawienie połączenie VPN wyłącznie za wiedzą i zgodą Zamawiającego.
   10. Wszystkie czynności serwisowe będą odbywały się wyłącznie w środowisku/infrastrukturze Zamawiającego.

\**UWAGA: brak potwierdzenia spełnienia przez Wykonawcę parametrów i warunków dla urządzenia wymaganych przez Zamawiającego będzie traktowane jako brak danego parametru i będzie skutkowało odrzuceniem oferty.*

*„Oświadczamy, że oferowane urządzenia spełniają wymagania techniczne, zawarte w powyższym opisie, są kompletne, fabrycznie nowe i będą gotowe do użytku bez żadnych dodatkowych zakupów.”*

……….......…..……dnia…………… ...................................................

[*podpis elektroniczny osoby uprawnionej]*