Znak sprawy: ZTM.DU.3310.1.2019

Załącznik nr 1 do Umowy ……
z dnia ……

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest zakup 1 zestawu licencji dla 220 stacji roboczych na oprogramowanie Axence nVision, moduły: DataGuard, Users oraz Network, przeznaczone do monitorowania i ochrony danych przed „wyciekiem", aktywności użytkowników oraz infrastruktury.

Informacje dotyczące przedmiotu zamówienia:

I. W ramach oferty Wykonawca gwarantuje:

- wieczystą licencje na oprogramowanie dla Zamawiającego,
- moduł Network dla nielimitowanej liczby monitorowanych urządzeń,
- instalację wielu zdalnych konsol administracyjnych Axence nVision,
- 12 miesięcy Umowy Serwisowej (aktualizacje i pomoc techniczna),
- możliwość przedłużenia Umowy Serwisowej na kolejne 12 miesięcy w cenie 20% wartości licencji przy zachowaniu ciągłości (opcjonalnie),
- dostępność oprogramowania Axence nVision w dowolnej konfiguracji modułowej (funkcjonalnej) według rzeczywistych indywidualnych potrzeb użytkownika,
- możliwość dokupienia modułów (rozszerzenia funkcjonalności) oraz zwiększenia liczby zarządzanych stacji roboczych w ramach jednej licencji w dowolnym czasie.

II. Oferowane oprogramowanie powinno spełniać następujące minimalne wymagania:

1. Licencja obejmuje moduły oprogramowania dla serwera zarządzającego, zdalnych konsoli oraz agentów.
2. Komunikacja pomiędzy serwerem a Agentami i konsolami nawiązywana powinna być przy użyciu szyfrowanego protokołu TLS w wersji minimum 1.2.
3. Moduły oprogramowania umożliwiają kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomoc w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem.
4. Dane dotyczące aktywności pracownika na komputerze, czyli historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp. Powinny być odseparowane od danych stricte technicznych i mają być grupowane w osobnym, dedykowanym oknie. Pozwala to na, zgodnie z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.
5. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, ma być objęty kontrolą na poziomie wybranych Administratorów – w programie ma być możliwość nadawania kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników.
6. Program ma być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą

usunięcia, nawet jeśli użytkownik ma prawa administratora.

7. Program ma być dostępny w języku polskim i angielskim wraz z Podręcznikiem Użytkownika w formie cyfrowego podręcznika w formacie PDF oraz opcjonalnie strony internetowej.

8. Program powinien posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

9. W zakresie ochrony danych przed wyciekiem poprzez blokowanie urządzeń.

   9.1. Blokowanie urządzeń i nośników danych.

   9.2. Program powinien posiadać możliwość zarządzania prawami dostępu do wszystkich urządzeń wyjścia i wejścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.

   9.3. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.

   9.4. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.

   9.5. Zarządzanie prawami dostępu do urządzeń:

      a) Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.

      b) Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive, dysków itp. - urządzenia prywatne są blokowane.

      c) Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.

      d) Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.

   9.6. Audyt operacji na urządzeniach przenośnych:

      a) Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.

      b) Podłączenie/odłączenie urządzenia przenośnego.

   9.7. Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.

10. W zakresie obsługi użytkowników musi umożliwić monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

      a) faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),

      b) procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,

      c) rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona),

      d) informacji o edytowanych przez użytkownika dokumentach,

e) historii pracy (cykliczne zrzuty ekranowe).

f) listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt),

g) transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),

h) wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,

i) nagłówków przesyłanej poczty e-mail.

Ponadto program musi posiadać możliwość:

a) blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danej stacji roboczej z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych subdomen (np. *.domena.pl),

b) blokowania ruchu na wskazanych portach TCP/IP,

c) blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,

d) wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia,

e) możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie,

f) mechanizm blokowania uruchamiania aplikacji.

2. Monitorowanie infrastruktury (bezagentowo), które obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

a) wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping),
b) wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci,
c) wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie,
d) serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program musi monitorować czas ich odpowiedzi i procent utraconych pakietów.
e) Serwerów pocztowych:
   - program powinien monitorować zarówno serwis odbierający, jak i wysyłający pocztę,
   - program musi mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),

- program powinien mieć możliwość wykonywania operacji testowych,
- program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa,

f) monitorowania serwerów WWW i adresów URL,
g) obsługi szyfrowania SSL/TLS w powiadomieniach e-mail,
h) obsługi urządzeń SNMP wspierających SNMP v1/2/3 (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.),
i) obsługi komunikatów syslog i pułapek SNMP,
j) monitoringu routerów i przełączników wg:
   - zmian stanu interfejsów sieciowych,
   - ruchu sieciowego,
   - podłączonych stacji roboczych,
   - ruchu generowanego przez podłączone stacje robocze.
k) serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie.
l) wydajności systemów Windows: obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy.