Załącznik nr 6.4. do SWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (SOPZ)

Zadanie nr 4: Zakup licencji antywirusa

Obecne rozwiązanie: XCITIUM CLIENT SECURITY
ilość licencji: 200
Termin: licencja lub dostęp do dnia 30.06.2026 r.
Zamawiający dopuszcza zastosowanie rozwiązań równoważnych, zgodnych z opisem przedmiotu zamówienia, pod warunkiem, że zapewniona zostanie pełna funkcjonalność

1. Opis i minimalne parametry:

2.	Konsola zarządzająca	• Konsola web administratora powinna znajdować się w chmurze producenta znajdującej się na terenie Unii Europejskiej • Konsola web administratora musi posiadać możliwość wyboru języka polskiego • Konsola web musi umożliwiać zarządzanie stacjami roboczymi oraz serwerami i urządzeniami mobilnymi poprzez tą samą konsolę zarządzającą. • Konsola web musi posiadać możliwość tworzenia grup i polityk dla stacji. • Konsola web musi umożliwiać bezpieczne logowanie do konsoli zarządzającej po protokole HTTPS z certyfikatem. • Konsola web musi umożliwiać dwuetapową autoryzację logowania na minimum 2 sposoby. • Konsola web musi umożliwiać wykonanie instalacji oprogramowania firm trzecich zdalnie z konsoli na stacjach bezpośrednio z bezpiecznego repozytorium dostawcy rozwiązania antywirusowego. • Konsola web musi mieć możliwość zalogowania się kilku administratorom jednocześnie. • Konsola web musi posiadać zintegrowany moduł umożliwiający zdalne połączenie z graficznym pulpitem zdalnym przez dedykowaną aplikację dla komputerów/serwerów znajdujących się w sieci LAN i poza nią bez potrzeby tworzenia tuneli VPN każdej stacji komputera/serwera/Windows. • Konsola web musi mieć funkcję tworzenia raportów o stacjach w konsoli. • Konsola web musi mieć funkcję logów wykonywanych czynności przez administratorów konsoli.

	Agent ochrony konsoli – oprogramowanie antywirusowe	• Program antywirusowy powinien mieć obsługę w języku polskim. • Program antywirusowy powinien mieć obsługę w języku polskim. • Platforma powinna obsługiwać systemy operacyjne wymienione poniżej lub nowsze: macOS: 13.x, 14.x MS Windows (stacje klienckie): Windows 10 x64 Windows 11 x64 MS Windows (wersja serwerowa): Windows Server 2019 Windows Server 2022 Linux Latest Ubuntu 24.04 x64 Latest Debian 10.x x64 Latest CentOS 8.x x64 • Rozwiązanie powinno działać na komputerach wyposażonych minimalnie w: 512 MB dostępnej pamięci RAM 1 GB miejsca na dysku twardym dla wersji 32-bitowej i 64-bitowej • Instalacja oprogramowania musi być możliwa poprzez Active Directory, grupy robocze, poprzez sieć, pobranie paczki MSI i za pomocą dystrybucji przez pocztę e-mail. • Ochrona poczty - antywirus musi chronić stacje poprzez uruchamianie nieznanych oraz niebezpiecznych załączników w środowisku wirtualnym na stacji takim jak lokalna i automatyczna piaskownica (auto-sandbox). • Program antywirusowy musi posiadać możliwość skanowania wybranych plików, folderów/katalogów (również skompresowanych), a także całych dysków (w tym sieciowych) czy partycji. • Program antywirusowy musi posiadać możliwość skanowania dowolnego zasobu podłączonego do stacji roboczej np.: dyski zewnętrzne, pamięci USB • Program antywirusowy powinien posiadać filtering URL umożliwiający blokowanie konkretnych stron internetowych. • Program antywirusowy musi posiadać moduł antywirusowy chroniący w czasie rzeczywistym. • Program antywirusowy musi posiadać moduł sprawdzający reputację plików w chmurze.

		• Program antywirusowy musi posiadać dwukierunkowy konfigurowalny z konsoli web firewall z możliwością tworzenia polityk globalnych i z podziałem na aplikacje.
		• Program antywirusowy musi posiadać moduł HIPS (Host Intrusion Protection System – ochrona antywłamaniowa).
		• Program antywirusowy musi posiadać moduł automatycznej piaskownicy (autosandbox), odizolowanego środowiska wirtualnego, w którym zasoby są emulowane dla obiektów w nim umieszczonych. Dodatkowo cały proces izolacji dzięki temu modułowi musi odbywać się lokalnie, na stacji roboczej. Całe środowisko wirtualne musi być odwzorowaniem 1:1 z systemem operacyjnym. Użytkownik powinien móc pracować w zwirtualizowanym środowisku, bez możliwości zapisu na stacji poza środowiskiem wirtualnym.
		• Program antywirusowy musi posiadać możliwość uruchomienia dowolnego pliku/programu w automatycznej piaskownicy (auto-sandbox) na żądanie użytkownika (manualnie).
		• Program antywirusowy musi umożliwiać użytkownikowi wysłanie podejrzanego obiektu do producenta oprogramowania antywirusowego w celu jego analizy. Funkcja ta powinna być dostępna z interfejsu programu antywirusowego.
		• Podczas pracy komputera Program musi automatycznie skanować:
		  ○ pliki uruchamiane, otwierane,
		  ○ pliki kopiowane lub przenoszone,
		  ○ pliki tworzone,
		  ○ pliki pobierane z Internetu po protokole HTTP/HTTPS.
		• W przypadku wykrycia wirusa program musi posiadać możliwość automatycznego poddawania kwarantannie podejrzanych obiektów oraz opcję przywrócenia z kwarantanny usuniętych obiektów.
		• Program antywirusowy musi posiadać funkcję dodawania wyjątków do modułu antywirusowego, automatycznej piaskownicy (auto-sandbox) czy modułu HIPS.
		• Program antywirusowy posiada zintegrowaną funkcję blokowania urządzeń zewnętrznych / przenośnych przed odczytem, edycją i zapisem plików w tym samym czasie.
		• Program antywirusowy posiada zintegrowaną funkcję blokowania jedynie zapisu plików na urządzeniach zewnętrznych / przenośnych.
		• Program antywirusowy powinien posiadać możliwość aktualizowania baz danych antywirusowych ręcznie, nawet jeśli komputer nie będzie miał dostępu do Internetu.

		• Program antywirusowy posiada zintegrowaną funkcję skanowania i ochrony plików pod kątem danych wrażliwych (DLP).

2. Rozwiązania równoważne:

   1) jeżeli Zamawiający w opisie przedmiotu zamówienia wskazał znaki towarowe, patenty lub pochodzenia, źródła lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, dopuszcza się zaoferowanie rozwiązań równoważnych opisanym, pod warunkiem zachowania przez nie takich samych minimalnych parametrów technicznych, jakościowych oraz funkcjonalnych itp.,

   2) Wykonawca, który powołuje się na rozwiązania równoważne, jest zobowiązany wykazać, że oferowane przez niego rozwiązanie spełnia wymagania określone przez Zamawiającego. W takim przypadku, Wykonawca załącza do oferty wykaz rozwiązań równoważnych wraz z jego opisem lub normami,

   3) w przypadku, gdy w opisie przedmiotu zamówienia znajdą się odniesienia do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w 5 art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy Prawo zamówień publicznych, Zamawiający dopuszcza rozwiązania równoważne opisywanym.

Zgodnie z art. 8 ust. 5 Ustawy o systemie oceny zgodności (t.j. Dz.U. z 2021 r. poz. 1344 z późn. zm.) zabrania się wprowadzania do obrotu lub oddawania do użytku wyrobu nieposiadającego oznakowania zgodności, jeżeli wyrób ten podlega takiemu oznakowaniu. W związku z powyższym Zamawiający będzie wymagał od Wykonawcy stosownego oświadczenia w stosunku do wyrobów, które podlegają takiemu oznakowaniu. Zgodnie z zapisami umowy, Wykonawca przedstawi dokumenty dotyczące materiałów i urządzeń (certyfikat zgodności z Polską Normą lub aprobatę techniczną), w terminie co najmniej 7 dni kalendarzowych przed zamiarem ich wbudowania. Materiały mogą zostać zabudowane po uzyskaniu akceptacji Inspektora nadzoru.