Załącznik nr 1

dot. sprawy nr. 181168/2023

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa oprogramowania do zarządzania i kontroli dostępu do sieci dla Uniwersytetu Śląskiego" – 1 szt.

Parametry wymagane	Parametry oferowane
SYSTEM KONTROLI I ZARZĄDZANIA DOSTĘPEM DO SIECI (SYSTEM NAC) Przedmiotem postępowania jest dostarczenie centralnego systemu kontroli i zarządzania dostępem do sieci LAN oraz WLAN współpracującego z posiadaną przez Zamawiającego infrastrukturą dostępową. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu NAC były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy wirtualne wraz z odpowiednio zabezpieczonym systemem operacyjnym wraz z wszystkimi niezbędnymi licencjami (również systemu operacyjnego) niezbędnymi do instalacji w ramach klastra wysokiej dostępności złożonego z co najmniej 12 serwerów fizycznych. Platformy wirtualne muszą wspierać następujące rodzaje hypervisorów: Vmware vSphere, Microsoft Hyper-V oraz Proxmox wykorzystywane przez Zamawiającego. W ramach postępowania muszą zostać dostarczone wszystkie elementy fizyczne lub wirtualne niezbędne do monitorowania i zarządzania kontrolą dostępu co najmniej 3000 urządzeń w co najmniej 30 segmentach sieci zlokalizowanych w 10 lokalizacjach fizycznych. **Architektura** 1. System musi umożliwiać instalację rozproszoną na wielu serwerach fizycznych lub wirtualnych w celu zapewnienia wysokiej niezawodności i możliwości	

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

stopniowego zwiększania wydajności systemu (skalowanie).

2. Elementy Systemu muszą umożliwiać klastrowanie active-passive. W ramach postępowania System musi zostać dostarczony w wersji redundantnej.
3. System NAC musi pracować w trybie out-of-band, tj. realizować wszystkie wymagane funkcje bez konieczności analizy ruchu sieciowego (na porcie SPAN, inline).
4. Wszystkie elementy Sytemu powinny być zarządzane centralnie.
5. System i jego wszystkie funkcje muszą w pełni współpracować z urządzeniami Zamawiającego (tj. można na nich wydawać polecenia konfiguracyjne z poziomu systemu kontroli i zarządzania dostępem do sieci):
    - Firewalle:
        a) PaloAlto PA5220,
        b) Fortigate 500E,
        c) Stormshield,
    - Przełączniki:
    - Kontroler sieci bezprzewodowej i zarządzane przez niego urządzenia Access Point:
    - Domena Active Directory.

Funkcje Systemu

1. System musi umożliwiać uwierzytelnienie użytkowników i urządzeń podłączanych do sieci lokalnej LAN i sieci bezprzewodowej WLAN z wykorzystaniem:
    - standardu 802.1X
    - adresu MAC urządzenia
    - formularza webowego (captive portal) z wykorzystaniem LDAP lub przy pomocy loginu i hasła z lokalnej bazy danych użytkowników w Systemie.
2. System musi obsługiwać uwierzytelnianie w oparciu o: wbudowany serwer RADIUS, zewnętrzny serwer Radius, protokół LDAP, jak również w oparciu o wewnętrzną bazę użytkowników i urządzeń.
3. System musi obsługiwać autoryzację w oparciu o adresy MAC definiowane w wewnętrznej bazie z wykorzystaniem protokołu RADIUS.
4. System musi zapewniać automatyczne wykrywanie urządzeń końcowych i śledzenie ich

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, LDAP) lub żądania RADIUS pochodzących z przełączników dostępowych. W ramach postępowania muszą zostać dostarczone wszystkie niezbędne elementy, które umożliwią realizację powyższej funkcji we wszystkich lokalizacjach i segmentach sieci.

5. System powinien logować i przetrzymywać we własnej bazie danych co najmniej następujące informacje:
    - adresy MAC przełączników, urządzeń końcowych i dostępowych,
    - adresy IP ww. urządzeń
    - identyfikatory i nazwy portów przełączników określające porty na przełącznikach i urządzeniach dostępowych do których podłączane są urządzenia końcowe
    - stan skanowania - wyniki skanowania urządzenia końcowego i jego ocena. w oparciu skanowanie przeprowadzone przy pomocy dostępnych w rozwiązaniu agentów
    - informacje o użytkownikach
    - nazwa użytkownika do którego przypisany jest urządzenie końcowe
    - nazwa zalogowego użytkownika na urządzeniu końcowym, jeśli wykonywana jest na nim autoryzacja
    - profil/rola jak została przydzielona urządzeniowi końcowemu przez System
    - data zarejestrowania urządzenia końcowego w Systemie
    - data ostatniego logowania urządzenia końcowego w sieci lub/i podłączenia
6. System musi umożliwiać tworzenie reguł autoryzacji (kontroli dostępu) opartych o złożone i wielowarunkowe polityki bezpieczeństwa. Powinny one obejmować co najmniej: lokalizacja urządzenia w sieci, przynależność do grupy administracyjnej, parametr opisujący urządzenie lub użytkownika.
7. System musi aktywnie zapobiegać przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych urządzeń końcowych i innych niechronionych urządzeń. Dla tak zdefiniowanych urządzeń końcowych muszą być zapewnione

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

mechanizmy automatycznej kwarantanny oraz blokowania. 8. System musi zapewniać możliwość powiadamiania poprzez SYSLOG oraz pocztę elektroniczną o sytuacjach krytycznych np. związanych z próbą nieautoryzowanego dostępu do sieci lub awarii wewnętrznych usług Systemu NAC. 9. System musi posiadać wewnętrzną bazę urządzeń. Baza musi umożliwiać wprowadzanie danych poprzez import danych, wprowadzanie danych z poziomu Systemu lub z wykorzystaniem API. 10. System musi wykorzystywać informacje zawarte w bazie urządzeń końcowych dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania oraz autoryzacji. 11. System musi posiadać bazę minimum 30 kategorii urządzeń końcowych. 12. System musi mieć możliwość klasyfikacji jednorazowej przy wstępnym uwierzytelnianiu/rejestracji bądź klasyfikacji wielokrotnej. Klasyfikacja urządzeń i użytkowników musi bazować na harmonogramie z częstotliwością w przedziale od kilku minut do kilku tygodni. 13. System musi umożliwiać wykonywanie na urządzeniach sieciowych skryptów CLI, które są elementem polityk bezpieczeństwa. 14. System musi obsługiwać telefony IP wraz z możliwością podłączenia do nich stacji końcowych (przez wbudowany przełącznik w telefonie) przypisując każdemu z urządzeń dedykowane polityki bezpieczeństwa. 15. System musi podejmować decyzję o przyłączeniu urządzeń końcowych do sieci poprzez ocenę ich zgodności ze zdefiniowanymi wymaganiami. Ocena zgodności musi być realizowana zarówno bez dedykowanego agenta instalowanego na stacji końcowej (za pomocą metod takich jak: WinRM, WMI) jak i z użyciem agenta. Ocena stanu stacji końcowych musi być możliwa zarówno w trybie „pre-connect" przed udzieleniem dostępu do sieci, jak i w trybie „post-connect – po udzieleniu dostępu do sieci. 16. Klasyfikacja urządzeń końcowych z użyciem agenta dedykowanego dla komputerów z systemem Windows i MAC OS X musi umożliwiać przeprowadzenie następujących testów:	

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

a. Sprawdzenie wersji agenta
b. Sprawdzenie wersji systemu operacyjnego,
c. Sprawdzenie obecności i stanu oprogramowania antywirusowego (niezainstalowany/zainstalowany, uruchomiona ochrona, zaktualizowany),
d. test zapory (włączona/wyłączona),
e. test poprawek do systemów Windows (sprawdzanie czy poprawka jest zainstalowana bądź nie),
f. test usługi Windows Update z opcją automatycznego naprawienia niezgodności
g. test obecności/niewystępowania pliku o określonej nazwie
h. test obecności procesu (uruchomiony/nieuruchomiony)
i. test rejestru dla systemów Windows (obecność klucza o zdefiniowanej nazwie, typie wartości i wartości, równy bądź różny zadanemu)
j. test stanu usługi (uruchomiona/nieuruchomiona)
k. test obecności aplikacji (sprawdzenie czy aplikacja zdefiniowanej nazwie jest zainstalowana)

17. Wykorzystywany przez system Agent nie może wprowadzać zmian w działaniu aplikacji lub procesów systemu operacyjnego.
18. System musi mieć możliwość przeprowadzania różnych metod testowania w zależności od lokalizacji urządzenia w sieci, przynależności do grupy administracyjnej, parametru opisującego urządzenie lub użytkownika.
19. Podczas oceniania urządzenia końcowego musi być możliwość określenia alternatywnej polityki dostępu do zasobów w przypadku braku zgodności.
20. System musi mieć możliwość przeniesienia urządzenia do kwarantanny w przypadku braku komunikacji z agentem.
21. Na urządzeniu podlegającym kwarantannie musi zostać wyświetlona informacja o fakcie przeniesienia urządzenia do kwarantanny oraz informacja z wytycznymi o działaniach jakie użytkownik urządzenia musi podjąć w celu usunięcia niezgodności.

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

22. Administrator musi mieć możliwość określenia poziomu niezgodności z politykami, po którym będzie następowało przeniesienia stacji do kwarantanny.
23. System musi zapewniać integrację z rozwiązaniami bezpieczeństwa (platformy Firewall, systemy SIEM, systemy Antymalware, systemy MDM) na potrzeby oceny stanu urządzeń końcowych oraz określenia ich zgodności z polityką bezpieczeństwa NAC. Ocena stanu stacji końcowych musi być możliwa zarówno w trybie „pre-connect" przed udzieleniem dostępu do sieci, jak i w trybie „post-connect – po udzieleniu dostępu do sieci.
24. System musi zapewniać integrację z platformami typu Firewall w ramach której:
    a. możliwy jest import stanu sesji urządzeń końcowych z platformy Firewall i wykorzystanie tych informacji jako danych wejściowych w konfiguracji metod profilowania urządzeń końcowych.
    b. możliwe jest wykorzystanie funkcji rozpoznawania urządzeń końcowych przez platformę Firewall jako daną wejściową w konfiguracji metod profilowania urządzeń końcowych.
25. System musi zapewniać integrację z serwerem wdrażania, zarządzania, rejestrowania i monitorowania urządzeń końcowych w ramach której:
    a. System NAC może gromadzić dane o urządzeniach końcowych (nazwa urządzenia końcowego, typ, system operacyjny, użytkownik, zgodność z polityką bezpieczeństwa)
    b. System NAC może wykorzystać zgromadzone dane do rejestracji urządzenia końcowego.

Profilowanie urządzeń

1. System musi umożliwiać rozpoznawanie rodzaju urządzeń podłączonych do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez analizę informacji pochodzących z co najmniej następujących źródeł: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta,

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

WinRM, WMI, Location, Agent, IP Range, Network Traffic. 2. System musi posiadać funkcję automatycznego profilowania urządzeń nie posiadających agenta 802.1x (suplikanta) na podstawie: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta, WinRM, WMI, Location, Agent, IP Range, Network Traffic i przyznawania dostępu do sieci na podstawie zdefiniowanych polityk dostępu do sieci. 3. System musi umożliwiać dodawania rozpoznanych urządzeń do grup systemowych. 4. System na podstawie rodzaju rozpoznanego urządzenia musi umożliwiać różnicowanie poziomu dostępu. 5. System musi rozpoznawać co najmniej następujące rodzaje urządzeń: • urządzenia z systemem Android, • urządzenia Apple (iPad, iPhone, iPod) • drukarki sieciowe, • telefony IP, • stacje robocza z systemem Microsoft Windows, • stacje robocza z systemem MAC OS, • stacje robocza z systemem Linux. 6. System musi posiadać funkcję wykrywanie nieautoryzowanych serwerów DHCP. 7. System musi posiadać funkcję wykrywania procesu NAT na urządzeniach końcowych. **Logowanie, Raportowanie i Alarmowanie** 1. System musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń). 2. System musi mieć możliwość generowania szczegółowego wykazu urządzeń podłączonych do sieci, zorganizowanego według typu urządzenia końcowego. 3. System musi rejestrować dane o atrybutach urządzeń końcowych i raportować zmiany w atrybutach np. przydział do VLAN-u, przyznany adres IP, klasyfikacja urządzenia w Systemie. 4. System musi zapewniać dane historyczne o zmianach stanu konfiguracji portów dostępowych.	

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

5. System musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania i procesem podłączanych urządzeń. Dane muszą być przechowywane i dostępne do analizy przez co najmniej 12 miesięcy.
6. System musi oferować możliwość tworzenia własnych szablonów raportów.
7. System musi umożliwiać logowanie do zewnętrznych serwerów logowania z wykorzystaniem Syslog.
8. System musi umożliwiać konfigurację generowanych alarmów i zautomatyzowanych akcji w oparciu o zdarzenia wewnętrzne np. w przypadku stwierdzenia zagrożenia na stacji, zablokowanie jej i powiadomienie administratora.
9. System musi umożliwiać przekazywanie informacji do systemów zewnętrznych poprzez mechanizm np. ODBC.
10. System NAC musi zapewniać integrację z modułem analizy i raportowania pochodzącym od tego samego producenta, w którym możliwe jest – oprócz logowania i raportowania – tworzenie reguł korelujących i alarmujących.

Zarządzanie systemem

1. System musi posiadać graficzny interfejs zarządzania – zarządzanie poprzez przeglądarkę internetową w wersji oferowanej przez producenta przeglądarki lub dedykowaną aplikację.
2. System musi umożliwiać uwierzytelnienie i autoryzację dostępu do interfejsu zarządzania w oparciu o wewnętrzną bazę użytkowników lub zewnętrzne repozytorium użytkowników (LDAP lub Radius).
3. System musi umożliwiać definiowanie zróżnicowanego poziomu dostępu do interfejsu zarządzania - RBA.
4. System musi umożliwiać zdefiniowanie co najmniej 3 administratorów z możliwością określenia praw dostępu do poszczególnych elementów systemu.
5. System musi umożliwiać personalizację wyglądu interfejsu zarządzania, w tym co najmniej zmianę koloru tła i czcionek, treści, grafiki.
6. System musi posiadać panel administracyjny, przedstawiający szczegółowy obraz stanu

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

zabezpieczeń podłączonych lub próbujących się podłączyć urządzeń końcowych.

Zarządzanie dostępem gościnnym

1. System musi umożliwiać przyznawanie dostępu gościnnego do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez wypełnienie formularza w portalu rejestracyjnym.
2. System musi umożliwiać realizację usług BYOD dla urządzeń prywatnych pracowników.
3. Funkcja portalu rejestracyjnego powinna działać bez udziału lub przy minimalnym udziale pracowników IT. System powinien posiadać możliwość delegowania uprawnień do akceptowania kont gości przez pracowników nieposiadających uprawnień administracyjnych w Systemie.
4. Wsparcie dla linków akceptacyjnych generowanych z portalu sponsorskiego.
5. Rejestracja gości powinna umożliwiać powiązanie z bramką SMS celem wysyłania PIN-ów weryfikacyjnych. Wymagana jest obsługa PIN-ów składających się ze znaków alfanumerycznych i znaków specjalnych.
6. System musi umożliwiać przyznanie dostępu czasowego dla gości.
7. System musi umożliwiać dopasowanie wyglądu portalu logowania gościnnego, w tym co najmniej zmianę logo strony logowania, zmianę koloru tła i czcionek, treści, grafiki.

Licencje i serwisy

1. W ramach postępowania koniecznym jest dostarczenie 3000 licencji umożliwiających uruchomienie wszystkich wyżej wymienionych funkcji z zastosowaniem agenta na stacjach końcowych, z założeniem że są one równocześnie podłączone do sieci lokalnej LAN i sieci bezprzewodowej WLAN.
6. Licencje w ramach rozwiązania powinny być dostarczone w modelu permanentnym. Zamawiający nie dopuszcza licencji bazujących na subskrypcji.
7. Dostarczony System NAC musi zawierać wszystkie niezbędne komponenty na których możliwa będzie licencyjna rozbudowa do min. 3000 urządzeń równocześnie podłączonych

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl

do sieci lokalnej LAN i sieci bezprzewodowej WLAN, z uwzględnieniem instalacji agentowej.

8. Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
9. System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

Opisy do wymagań ogólnych

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Uniwersytet Śląski w Katowicach
Dział Zarządzania Dostawami
ul. Bankowa 14, 40-007 Katowice
tel.: 32 359 13 63, e-mail: maria.rys@us.edu.pl
www.us.edu.pl