ZAŁĄCZNIK NR 1 DO SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

pn. Zakup sprzętu w ramach projektu pn.:
„Cyfrowe usługi publiczne w Gminie Braniewo II”

Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Warmińsko-Mazurskiego 2014-2020;
Oś Priorytetowa 3. Cyfrowy Region
Działanie 3.1 Cyfrowa dostępność informacji sektora publicznego
oraz wysoka jakość e-usług publicznych

Braniewo, lipiec 2023 r.

SPIS TREŚCI

1 OGÓLNE INFORMACJE

Projekt pn. „Cyfrowe usługi publiczne w Gminie Braniewo II" jest realizowany przez Gminę Braniewo. Głównym miejscem realizacji Projektu będzie siedziba Zamawiającego:
Urząd Gminy Braniewo, ul. Moniuszki 5, 14-500 Braniewo.

W ramach realizacji przedmiotowego Zamówienia zostanie wdrożony zintegrowany system teleinformatyczny umożliwiający świadczenie przez Zamawiającego e-usług na wysokim poziomie dojrzałości. Wdrożony system pozwoli na prowadzenie usług zgodnych z przepisami prawa dotyczącymi interoperacyjności, bezpieczeństwa oraz standardu dostępu dla niepełnosprawnych. Wprowadzony system będzie współpracował zarówno z komputerami typu desktop oraz urządzeniami mobilnymi typu laptop, tablet czy smartfon. W wyniku realizacji Projektu, Zamawiający zwiększy dostęp społeczeństwa do usług świadczonych drogą elektroniczną, zgodnych z obowiązującym prawodawstwem.

Przedmiot niniejszego postępowanie obejmuje zakup sprzętu i oprogramowania wymienionego poniżej:

1. Szafa Rack – 1 szt.
2. Macierz – 1 szt.
3. Serwer Kopii Zapasowych – 1 szt.
4. Akcesoria SFP+ - 5 szt.
5. Pamięć RAM – typ I – 1 szt.
6. Pamięć RAM – typ II – 4 szt.
7. Baterie UPS – 2 szt.
8. Przełącznik Główny 10GB Rack – 1 szt.
9. Przełącznik dostępowy 1GB Rack – 2 szt.
10. System Antywirusowy – 35 szt.
11. Tablet – 18 szt.
12. Doposażenie eRada – kamera – 1 szt.

Opisane poniżej wymagania stanowią zakres minimalnych oczekiwań Zamawiającego dla przedmiotu dostawy.

OGÓLNE ZASADY RÓWNOWAŻNOŚCI ROZWIĄZAŃ:

1. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same

funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.

2. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych, Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych nie gorszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający informuje, że w takiej sytuacji przedmiotowe zapisy są jedynie przykładowe i stanowią wskazanie dla Wykonawcy, jakie cechy powinny posiadać składniki użyte do realizacji przedmiotu zamówienia. Zamawiający zgodnie z art. 99 ust. 6 ustawy z dnia 24 października 2019 r. Prawo zamówień publicznych, zwanej dalej ustawą, dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.), jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów/produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach.

3. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia, o których mowa w art. 101 ust. 1-3 ustawy, zgodnie z art. 101 ust.4 ustawy dopuszcza rozwiązania równoważne opisywanym. Zgodnie z art. 101 ust. 5 ustawy – Zamawiający nie może odrzucić oferty tylko dlatego, że oferowane roboty budowlane, dostawy lub usługi nie są zgodne z normami, ocenami technicznymi, specyfikacjami technicznymi i systemami referencji technicznych, do których opis przedmiotu zamówienia się odnosi, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.

1.1 MIEJSCE REALIZACJI DOSTAW I USŁUG

Dostawy i usługi będą realizowane w siedzibie Zamawiającego, tj. w Urzędzie Gminy Braniewo.

Dokładny adres realizacji projektu

Urząd Gminy Braniewo

ul. Moniuszki 5

14-500 Braniewo

Szczegółowy zakres dostawy, usług oraz prac do wykonania został przedstawiony w dalszej części niniejszego załącznika.

1.2 Termin i Harmonogram Wykonania Zamówienia

Wymagany termin wykonania Zamówienia – **maksimum 30 dni kalendarzowych od dnia podpisania umowy lub krócej zgodnie ze złożoną ofertą**.

1.3 Ogólne informacje dotyczące zamówienia

W tabeli poniżej przedstawiono wykaz sprzętu i licencji (oprogramowania), jakie mają zostać dostarczone w ramach przedmiotowego zamówienia oraz okres minimalnej gwarancji lub okres na jaki ma zostać udzielona licencja.

W przypadku sprzętu w pozycjach w których wpisano 36 lub 48 lub 60 m-cy, Wykonawca ma możliwość w formularzu oferty zaoferować okres gwarancji o długości 36 lub 48 lub 60 m-cy.

Są to kryteria punktowe opisane w Specyfikacji Warunków Zamówienia.

Nazwa usługi i produktu	jednostka	ilość	Rozdział OPZ	Gwarancja / licencja min.
Szafa Rack	1	szt.	2.1	36 m-cy lub 48 m-cy lub 60 m-cy
Macierz	1	szt.	2.2	36 m-cy lub 48 m-cy lub 60 m-cy
Serwer Kopii Zapasowych	1	szt.	2.3	36 m-cy lub 48 m-cy lub 60 m-cy
Akcesoria SFP+	5	szt.	2.4	36 m-cy lub 48 m-cy lub 60 m-cy
Pamięć RAM – typ I	1	szt.	2.5	36 m-cy lub 48 m-cy lub 60 m-cy
Pamięć RAM – typ II	4	szt.	2.6	36 m-cy lub 48 m-cy lub 60 m-cy
Baterie UPS	2	szt.	2.7	60 m-cy
Przełącznik Główny 10GB Rack	1	szt.	2.8	60 m-cy
Przełącznik dostępowy 1GB Rack	2	szt.	2.9	60 m-cy
System Antywirusowy	35	szt.	2.10	60 m-cy
Tablet	18	szt.	2.11	36 m-cy lub 48 m-cy

				lub 60 m-cy
Doposażenie eRada – kamera	1	szt.	2.12	36 m-cy lub 48 m-cy lub 60 m-cy

2 OGÓLNE WYMAGANIA OPROGRAMOWANIA I ROZWIĄZAŃ

W ramach zamówienia należy dostarczyć opisany poniżej sprzęt i oprogramowanie oraz wykonać następujące prace:

1. Szczegółowy opis montażu elementów wyposażenia serwerowni.
2. Montaż i konfiguracja sprzętu muszą być wykonane w godzinach i dniach wolnych od pracy Zamawiającego, w godzinach 16:00 do 6:00 lub w weekendy. W terminach uzgodnionych z Zamawiającym.
3. Ilość komputerów/użytkowników dodawanych do AD – 30 szt.
4. Macierz dyskowa musi być zainstalowana (dyski zamontowane) i skonfigurowana do pracy wg ustaleń z zamawiającym, wykonawca przeprowadzi szkolenie z obsługi macierzy.
5. Macierz oraz NAS muszą być zainstalowane i skonfigurowane, gotowe do pracy wg ustaleń z zamawiającym. W odniesieniu do NASa Wykonawca przeszkoli w zakresie obsługi i administracji serwera NAS administratora sieci. Serwer NAS ma umożliwiać między innymi archiwizację przyrostową i pełną serwerów zainstalowanych w budynku urzędu.
6. Macierz musi zostać zainstalowana w szafie RACK.
7. Skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzenia pozwalające na rozpoczęcie pracy.
8. Macierz musi mieć zainstalowany zaproponowany system oraz załączone oprogramowanie i być skonfigurowana do pracy. Serwer NAS będzie wykorzystywany do celów backupu oraz do zabezpieczenia przed ransomware, co należy skonfigurować.
9. System należy zainstalować i skonfigurować na systemie macierzowym zgodnie z zaleceniami zamawiającego oparty na platformie wirtualizacji XCP. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
10. W urządzeniach Aktywnych Wykonawca nada IP służące do zarządzania, zamienić standardowe Hasła na wskazane przez Zamawiającego, konfiguracyjnie odseparować sieci produkcyjną od sieci zarządzalnej.
11. Wykonawca dodatkowo:
    a. Zapewni połączenia pomiędzy urządzeniami typu: przełącznik agregacyjny i dostępowe, macierz, serwer backupowy, wykorzystując wkładki światłowodowe 10GE z patchcordami światłowodowymi kompatybilnymi zaoferowanymi wkładkami

lub DAC zapewniając maksymalną prędkość i przepustowość 10Gb/s. UTM połączy poprzez 1GE RJ45

b. Dokona zainstalowania i skonfigurowania DC wraz z kontrolerem zapasowym DC
c. Utworzy i skonfiguruje role: WSUS, DHCP, SERWER PLIKÓW, NTP,
d. Przeprowadzi audyt istniejących polityk oraz wdroży rekomendowane polisy bezpieczeństwa w AD DC, switchach oraz w UTM.
e. Utworzy 3 przykładowe polityki GPO.
f. Uruchomi dodatkowe usługi – zgodnie z potrzebami Zamawiającego.
g. Przeprowadzi instruktaż dla Administratora.
h. Zainstaluje wszystkie zamówione programy, zaktualizuje do najnowszej wersji.

Dostarczany sprzęt i wyposażenie musi pochodzić z oficjalnego polskiego kanału dystrybucji.

2.1 SZAFA RACK – 1 SZT.

Lp.	Minimalne wymagania
1.	Rozmiar: 42U
2.	Wymiary: 600 x 1000 mm.
3.	Nośność statyczna: 800 kg
4.	Wyposażenie: 2 listwy zasilające 6-portowe shuko dwubiegunowym wyłącznikiem 1U długość kabla 1.5m , 2x półka, panel wentylacyjny z 4 wentylatorami, Wbudowany czujnik temperatury, 1 U, 2 półki dostosowane do szafy głębokość 750mm
5.	Drzwi przednie perforowane szklane z zamkiem, wentylowane
6.	Drzwi boczne stalowe demontowane na zatrzaskach
7.	Drzwi tylne stalowe wentylowane z zamkiem
8.	Otwory na przewody: 4 przepust kablowy w podłodze i w suficie
9.	Otwory wentylacyjne
10.	Kolor wszystkich części szafy i akcesoriów: czarny
11.	Stopień Ochrony IP20

2.2 MACIERZ – 1 SZT.

Lp.	Minimalne wymagania
1.	Obudowa: max. 3U wraz z szynami umożliwiającymi montaż serwera w szafie rack,
2.	Procesor wielordzeniowy, o minimalnej wydajność pojedynczego CPU min. 6 800 punktów w teście wydajności CPU PassMark Performance Test (Pomiar średni - Average CPU Mark) - stan nie wcześniej niż dzień ogłoszenia postępowania. **Załączyć wydruk do Oferty ze strony https://www.cpubenchmark.net.**
3.	Pamięć systemowa: min. 32GB na kontroler, 64GB DDR4 ECC na urządzenie
4.	Pamięć NVRAM (write cache) z podtrzymaniem bateryjnym
5.	Ilość kontrolerów: min, 2 w trybie pracy- Active - Active
6.	Pamięć flash min.4 GB
7.	Wnęka dysków – min. 16 x 3,5” SAS 6Gb/s 12Gb/s
8.	Port LAN – min. 4x 10 GbE SFP+
9.	Port LAN – min. 3x min. 1 GbE RJ45
10.	Port USB – min. 4 x USB 3.1
11.	Zasilacz nadmiarowy/wymieniany podczas pracy; 2 x min. 750 W
12.	Obsługiwany system plików - dyski wewnętrzne: ZFS
13.	Obsługa sieci: TCP/IP (IPv4 IPv6) 10 Gb/s z obsługą ramek Jumbo Nadmiarowość połączeń (LACP, Load Balance, Failover, Round Robin) Klient DHCP Protokoły: SMB2/SMB3, NFS v3/NFS v4, FTP, FTPS, TFTP, HTTP, HTTPS, SSH, iSCSI, SNMP, SMTP i SMSC Wsparcie iSER

14.	Możliwość tworzenia połączeń sieciowych: fail-over, load balancing, agregacji
15.	Zainstalowane: • min. 2 dyski o pojemności min. 480GB SSD SAS zgodne ze stroną kompatybilności producenta. • min. 5 dysków o pojemności min. 3,84 TB SSD SAS 12 Gb/s. Dyski twarde zgodne ze stroną kompatybilności producenta. Dopuszcza się rozwiązanie równoważne umożliwiające osiągnięcie zakładaną minimalna sumaryczną pojemność dysków przy zachowaniu prędkości 12Gb/s. • min. 6 dysków o pojemności min. 14 TB SAS 12 Gb/s 7200 RPM, bufor 256 MB, czas pracy MTBF 2 000 000. Dyski twarde zgodne ze stroną kompatybilności producenta. Dopuszcza się rozwiązanie równoważne umożliwiające osiągnięcie zakładaną minimalna sumaryczną pojemność dysków przy zachowaniu prędkości 12Gb/s.
16.	Zarządzanie przestrzenią dyskową • Monitor wykorzystania zasobów • Obsługa RAID 0, 1, 5, 50, 6, 60, 10, RAIDTP, Triple Mirror • Obsługa puli dyskowych • Globalny dysk zapasowy • Pamięć podręczna odczytu konfigurowalna na dyskach SSD • Foldery udostępniane/LUN z thin provisioning • LUN z natychmiastowym przydzielaniem przestrzeni • Quota na udział • Odzyskiwanie przestrzeni • Obsługa migawek dla udziałów i LUN, • Menadżer migawek, klonowanie migawek • Deduplikacja dla folderów udostępnionych i LUN • Kompresja dla folderów udostępnionych i LUN • Wsparcie dla WORM (Write Once Read Many) dla folderów udostępnionych • Rozbudowa LUN online • Rozszerzanie puli pamięci online • SMART dysku twardego • Przywracanie RAID • Sumy kontrolne dla danych
17.	Certyfikaty:

	Macierz musi być wyprodukowana zgodnie z normą ISO-9001 oraz ISO-14001. Macierz musi posiadać deklaracje CE. **Dokumenty potwierdzające spełnianie powyższych wymogów należy załączyć do oferty.**
18.	W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym gwarancją, uszkodzony dysk twardy pozostaje u Zamawiającego.

2.3 SERWER KOPII ZAPASOWYCH – 1 SZT.

Lp.	Minimalne wymagania
1.	Obudowa: max. 2U wraz z szynami umożliwiającymi montaż serwera w szafie rack,
2.	Procesor wielordzeniowy, o minimalnej wydajność pojedynczego CPU min. 1100 punktów w teście wydajności CPU PassMark Performance Test (Pomiar średni - Average CPU Mark) - stan nie wcześniej niż dzień ogłoszenia postępowania. **Załączyć wydruk do Oferty ze strony https://www.cpubenchmark.net.**
3.	Pamięć systemowa: min. 8GB DDR4
4.	Pamięć flash min. 512 MB
5.	Wnęka dysków – min. 12 x 3,5” SATA 6Gb/s
6.	Port LAN – min. 2x 10 GbE SFP+
7.	Port LAN – min. 2x min. 1 GbE RJ45
8.	Port USB – min. 4 x USB 3.2
9.	Zasilacz nadmiarowy/wymieniany podczas pracy; 2 x max. 250 W
10.	Funkcje hot swap RAID 0/1/5/6/10. Przywracanie RAID. Migracja Poziomów RAID
11.	Kopia na dyski zewnętrzne i inne urządzenia
12.	Możliwość tworzenia połączeń sieciowych: fail-over, load balancing, agregacji
13.	Zainstalowane:

	• min. 2 dyski o pojemności min. 250GB SSD NVMe M.2, • min. 10 dysków o pojemności min. 10TB SATA 6 Gb/s 7200 RPM, bufor 256 MB, czas pracy MTBF 2 000 000. Dyski twarde zgodne ze stroną kompatybilności producenta. Dopuszcza się rozwiązanie równoważne umożliwiające osiągnięcie zakładaną minimalna pojemność dysków (dot. tylko pojemności dysków).
14.	Inne wymagania: • Buforowanie SSD, • Nadmiarowa alokacja SSD • Migawka/kopia zapasowa jednostek iSCSI LUN, • Kontroler domeny i serwer NTP, • Wolumin z elastycznym alokowaniem, • Jednostki iSCSI LUN oparte na blokach, • Odzyskiwanie miejsca, • Funkcja typu Storage Plug & Connect (iSCSI i CIFS), • Obsługa ACL na poziomie folderów współdzielonych, • Kopie Migawkowe, • Replikacja zdalna w czasie rzeczywistym, • Replikacja zdalna (rsync), • Oprogramowanie do tworzenia kopii zapasowych, • Obsługa etykiet woluminu na dyskach zewnętrznych, • Uwierzytelnianie AD, • Serwer i klient LDAP, • Powiadomienia (e-mail), • Kosz sieciowy, • SNMP, • Logowanie administratora przez Telnet i SSH.
15.	Certyfikaty: Serwer kopii zapasowych musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer kopii zapasowych musi posiadać deklaracje CE. **<u>Dokumenty potwierdzające spełnianie powyższych wymogów należy załączyć do oferty.</u>**
16.	W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym gwarancją, uszkodzony dysk twardy pozostaje u Zamawiającego.

2.4 AKCESORIA SFP+ - 5 SZT.

Lp.	Minimalne wymagania
1.	Modułu optyczny 10Gb/s SFP+ wraz z patchcordem światłowodowym 3m kompatybilne z zaoferowanymi modelami macierzy i serwera kopii zapasowych

2.5 PAMIĘĆ RAM – TYP I – 1 SZT.

Lp.	Minimalne wymagania
1.	Kość pamięci 64GB pamięci RAM do Servera Lenovo Thinksystem SR590 ECC LOAD REDUCED DDR4 4Rx4 2666MHz PC4-21300 LRDIMM

2.6 PAMIĘĆ RAM – TYP II – 4 SZT.

Lp.	Minimalne wymagania
1.	Kość pamięci RAM po 8GB do Servera KTRx4 ECC LOAD REDUCED DDR3 1333MHz PC3-10600 LRDIMM

2.7 BATERIE UPS – 2 SZT.

Lp.	Minimalne wymagania
1.	Kompatybilna z Ever Sinline 1200 Tower
2.	Żywotność: 60 m-cy
3.	Napięcie: 12V
4.	Typ: VRLA AGM
5.	Pojemność: 7Ah

2.8 PRZEŁĄCZNIK GŁÓWNY 10GB RACK – 1 SZT.

Lp.	Minimalne wymagania
1.	Przełącznik agregacyjny 10 gigabit Ethernet

2.	Porty przełącznika: minimum 24 porty 10GE SFP+; Porty SFP+ 10GE obsługujące moduły 1GE SFP; minimum 2 porty 40GE QSFP (z możliwością rozszycia każdego portu na 4x10G)
3.	Stackowanie: możliwość połączenia minimum 4 przełączników w stos za pomocą portów SFP+ lub QSFP bez dedykowanego okablowania
4.	Matryca przełączająca: minimum 656 Gbps
5.	Przepustowość pakietów: minimum 488 Mpps (dla pakietów 64Kb)
6.	Pojemność tablicy MAC: minimum 32k
7.	Ramka Jumbo: min 16k
8.	Ilość wpisów tablicy ACL: minimum 2,7k
9.	Ilość wpisów tablicy routingu: minimum 16k dla IPv4 z możliwością wykorzystania IPv6. Dopuszcza się rozwiązania współdzielące tablicę routingu dla IPv4 oraz IPv6 w maksymalnej proporcji 4:1.
10.	Ilość wpisów ARP: minimum 16k
11.	Ilość aktywnych IEEE802.1Q VLAN: minimum 4094
12.	Taktowanie procesora: minimum dual core 1,25 GHz
13.	Pamięć Flash: minimum 128MB
14.	Pamięć RAM: minimum 512MB
15.	Bufor pakietów: minimum 4MB
16.	Zasilanie urządzenia: wbudowany zasilacz 230V AC wraz z wbudowanym redundantnym zasilaczem 48 VDC
17.	Certyfikaty bezpieczeństwa: CE, RoHS
18.	Zabezpieczenie przeciwprzepięciowe: 6KV
19.	Algorytm pracy: Storage and forwarding
20.	Ruting L3: Static Routing, RIPv1/v2, RIPng, OSPFv2/v3, BGP4, BGP4+, OSPF multiple process, LPM Routing, Policy-based Routing (PBR) IPv4/IPv6, VRRP, IPv6 VRRPv3, URPF IPv4/IPv6,

	ECMP, BFD, Static Multicast Route, Multicast Receive Control
21.	Obsługa VLAN: Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ
22.	Obsługa spanning tree: IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding, Loopback Detection, Fast Link
23.	Protekcja ringowa: ITU-T G.8032
24.	Agregacja LACP: IEEE 802.3ad (LACP), minimum 128 grup per urządzenie oraz minimum 8 portów per grupa, load balance
25.	Funkcje QoS: 8 queues per port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, Queuing Method: Strict Priority, Weighted Round Robin, Weighted Deficit Round Robin, Strict priority in Weighted Round Robin, DNS Client, DNS Relay
26.	Bezpieczeństwo: Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN
27.	Listy kontroli dostępu: IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, ACL on VLAN interface, Rules can be configured to port, VLAN, VLAN routing interfaces
28.	Multicast: IGMP snooping v1/v2/v3 and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, PIM-SM, PIM-DM, PIM-SSM
29.	Zarządzanie: TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, CPU Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (min 4 urządzenia w stosie) – sprzętowa obsługa VSF
30.	Diagnostyka: sFlow, Traffic Analysis, RSPAN, VCT, DDM, Ping, Trace Route
31.	Obsługa DHCP: IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server
32.	Firmware oraz konfiguracja: oprogramowanie przełącznika (firmware) dostępny bez ograniczeń czasowych, przez cały okres cyklu życiowego urządzenia poprzez internet, wsparcie techniczne producenta lub dystrybutora bez konieczności wykupu dodatkowych usług, możliwość wgrania kilku plików z obrazem lub konfiguracją systemu, możliwość wgrania oprogramowania oraz konfiguracji poprzez TFTP/FTP
33.	4 Moduły optyczne 10Gb/s SFP+ wraz z patchcordem światłowodowym 3m kompatybilne z zaoferowanymi modelami macierzy i serwera kopii zapasowych.

2.9 PRZEŁĄCZNIK DOSTĘPOWY 1GB RACK – 2 SZT.

Lp.	Minimalne wymagania
1.	Porty przełącznika: minimum 24x 10/100/1000Base-T RJ45 oraz minimum 4x 1/10GBase-X SFP+
2.	Port konsolowy: RJ45 (RS-232)
3.	Port zarządzania: RJ45 (10/100Base-T RJ45)
4.	Port USB: minimum 1 port co najmniej w standardzie 2.0
5.	Szybkość przełączania: minimum 128Gb/s
6.	Przepustowość: minimum 95Mp/s (dla pakietów 64Kb)
7.	Bufor pakietów: minimum 1,5MB
8.	Ramki Jumbo: minimum 10k
9.	Tablica adresów MAC: minimum 16k
10.	Adresy MAC – Multicast: minimum 4k
11.	Tablica ACL: minimum 1k
12.	Tablica VLAN: minimum 4094
13.	Tablica routingu: minimum 1k dla IPv4 z możliwością wykorzystania IPv6. Dopuszcza się rozwiązania współdzielące tablicę routingu dla IPv4 oraz IPv6 w maksymalnej proporcji 4:1
14.	Taktowanie procesora: minimum 800MHz
15.	Pamięć Flash: minimum 128MB
16.	Pamięć RAM: minimum 512MB
17.	Temperatura pracy: zakres minimum 0°C - 50°C

18.	Wilgotność względna: zakres minimum 10% - 90% (bez kondensacji)
19.	Zasilanie: zabudowany zasilacz 230V AC
20.	Pobór mocy: maksymalnie 23W
21.	Zabezpieczenie przeciwprzepięciowe: minimum 6kV
22.	Wymiary: maksymalna: szerokość 440 mm, wysokość 44mm , głębokość 240mm
23.	Certyfikaty bezpieczeństwa: CE, RoHS
24.	Algorytm pracy: Store and Forward
25.	Obsługa VLAN: Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ
26.	DHCP: IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server
27.	Drzewo rozpinające: IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding, Fast Link, Loopback Detection
28.	Protekcja ringowa: ITU-T G.8032 – recovery time < 50ms
29.	Protokoły routingu: Static Routing, RIPv1/v2, RIPng, OSPFv2/v3, BGP4+, OSPF multiple process, LPM Routing, Policy-based Routing (PBR) IPv4/IPv6, VRRP, IPv6 VRRPv3, URPF IPv4/IPv6, ECMP, BFD, Static Multicast Route, Multicast Receive Control, Illegal Multicast Source Detect, GRE Tunnel
30.	Agregacja linków: IEEE 802.3ad (LACP), 128 groups per device / 8 ports per group, load balance
31.	Bezpieczeństwo: Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN
32.	Multicast: IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, PIM-SM, PIM-DM, PIM-SSM, IGMP authentication
33.	QoS: 8 queques per port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, Queuing Method: Strict Priority, Weighted Deficit Round Robin, Strict priority in Weighted Deficit Round Robin; DNS Client, DNS Relay

34.	Lista Kontroli Dostępu: IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN
35.	Diagnostyka: sFlow, Traffic Analysis, RSPAN, ERSPAN, VCT, Ping, Trace Route, Dying GASP
36.	Zarządzanie: TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (4 devices in one stack) – hardware stacking
37.	Oprogramowanie oraz wsparcie techniczne: oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług
38.	2 Moduły optyczne 10Gb/s SFP+ wraz z patchcordem światłowodowym 0,5m kompatybilne ze switchem agregacyjnym lub kabel HBA do połączenia switchy dostępowych z agregacyjnym.

2.10 System Antywirusowy – 35 szt.

Lp.	Minimalne wymagania
1.	Ochrona antywirusowa i antyspyware 1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim 3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi 4. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog 5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 6. Wbudowana technologia do ochrony przed rootkitami. 7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 10. Możliwość skanowania dysków sieciowych i dysków przenośnych. 11. Skanowanie plików spakowanych i skompresowanych.

	12. Możliwość dodawania wykluczeń na podstawie a) Plik b) Folder c) Rozszerzenie d) Proces e) Hash pliku f) Hash certyfikatu g) Nazwa zagrożenia h) Wiersz poleceń i) IP/maska 13. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express. 14. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 15. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 16. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 17. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta. 18. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 19. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać. 20. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS. 21. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 22. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło. 23. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie” możliwość wyświetlenia danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony. 24. W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji

	produktu i aktualnej wersji silników. 25. W GUI programu możliwość wyświetlenia kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia. 26. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 27. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 28. Praca programu musi być niezauważalna dla użytkownika. 29. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej. 30. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet. 31. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej. 32. Możliwość odblokowania ustawień programu po wpisaniu hasła 33. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu. 34. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie). 35. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu. 36. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.). 37. Funkcja Ochrony danych konfigurowana zdalnie przez administratora. 38. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows. 39. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego. 40. Wbudowany IDS. 41. Możliwość zainstalowania silnika pełnego lub lekkiego ze sprawdzaniem reputacji plików w chmurze. 42. Możliwość tworzenia list sieci zaufanych. 43. Możliwość dezaktywacji funkcji zapory sieciowej. 44. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. 45. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware. 46. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji. 47. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do

	zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa). 48. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups. 49. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego. 50. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać: a) Funkcję która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji: -Ochrony przeglądarki internetowej -Sieć i poświadczenia -Błędna konfiguracja systemu operacyjnego System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe. b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk. c) System który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie. d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania. e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach. f) System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie 51. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również: a) Możliwość wymuszenia funkcji DEP systemu Windows b) Możliwość wymuszenia relokacji modułów (ASLR) Uwaga: Ta warstwa zabezpieczeń dotyczy systemów opartych na systemie Windows. 52. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak: -Wczesny dostęp -Dostęp do poświadczeń

	-Wykrycie -Crimeware 53. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej. 54. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. Formaty plików jakie mogą być odzyskane: 3fr|ai|arw|bay|cab|cdr|cer|cr2|crt|crw|dcr|der|dgn|dll|dng|doc|docm|docx|dwg|dxf|dxg|eps|erf|exe|indd|ini|jpe|jpeg|jpg|mdf|mef|mrw|msg|msi|nef|nrw|odb|odc|odm|odp|ods|odt|orf|p12|p7b|p7c|pdd|pdf|pef|pem|pfx|png|ppt|pptm|pptx|psd|pst|ptx|py|r3d|raf|rtf|rw2|rwl|sr2|srf|srw|tsf|wb2|wpd|wps|x3f|xlk|xls|xlsb|xlsm|xlsx|xml| Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania.
2.	Stacje robocze i serwery 1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 3. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 6. Skanowanie plików spakowanych i skompresowanych. 7. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego. 8. Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu. 9. Produkt i sygnatury są aktualizowane nie rzadziej niż raz na godzinę. 10. Oprogramowanie posiada możliwość raportowania zdarzeń informacyjnych. 11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju. 12. Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych plików. 13. Program musi mieć wbudowany skaner wyszukiwania rootkitów. 14. Możliwość odblokowania ustawień programu po wpisaniu hasła. 15. Możliwość uruchomienia zadania skanowania z niskim priorytetem.

	16. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu). 17. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej. 18. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem 19. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym. 20. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
3.	Konsola zdalnej administracji 1. Dwa typy konsoli administracyjnej: • Konsola Cloud – serwer administracyjny po stronie producenta • Konsola On-premise – lokalny serwer administracyjny 2. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows. 3. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego. 4. Możliwość integracji Domeny Active Directory w obu typach konsoli. 5. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych. 6. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki). 7. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi 8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego. 9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internet 10. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej. 11. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa. 12. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej. 13. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv. 14. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.

	15. Możliwość generowania raportu co godzinę. 16. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu. 17. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej. 18. Możliwość dodania etykiety do stacji roboczej. 19. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej. 20. Możliwość przechowywania kwarantanny maksymalnie 180 dni 21. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać. 22. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny. 23. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej. 24. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym. 25. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania. 26. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy. 27. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie -Zakres adresów IP/IP -Adres bramy -Adres serwera WINS -Adres serwera DNS -Połączenie DHCP sufiksów DNS -Punkt końcowy może rozwiązać hosta -Typ sieci -Nazwa hosta 28. Integracja z serwerem Syslog. 29. Uwierzytelnienie dwuskładnikowe realizowane wyłącznie przez aplikację Google Authenticator 30. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni. 31. Możliwość zablokowania konta w konsoli jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem. 32. Funkcja pojedynczego logowania – Single Sign-on (SSO).

	33. Możliwość naprawy instalacji z poziomu konsoli. 34. Raport streszczający - Możliwość podglądu raportu który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak: - Zarządzane punkty końcowe - Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne - Pięć najczęściej blokowanych zagrożeń - Podział zagrożeń na urządzenia takie jak stacje robocze i serwery - Status incydentów bezpieczeństwa które wystąpiły - Stan modułów punktów końcowych - Ocena ryzyka firmy - Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa. - Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware 35. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak: a) Pakiety b) Sieć c) Kwarantanna d) Licencjonowanie e) Integracje f) Polityki g) Raporty h) Konta i) Firmy 36. Możliwość utworzenia reguły która będzie usuwała punkty końcowe z konsoli zarządzającej jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn które automatycznie będą usuwane oraz pozwala na określenie godziny kiedy te maszyny będą usuwane 37. Możliwość określenia własnego serwera NTP. 38. Integracja z vCenter Server. 39. Integracja z Xen Server. 40. Integracja z nutanix Prism Element. 41. Możliwość integracji z Amazon EC2 42. Intergracja z Azure.

	43. Pion firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej, dostępne muszą być opcje takie jak: a) Lotnictwo b) Rolnictwo c) Automotive d) Usługi komercyjne e) Doradztwo f) Energia g) Usługi finansowe h) Rząd i) Opieka zdrowotna j) Technologie k) Transport l) Non-profit m) Górnictwo n) Media 44. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta. 45. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą. 46. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS 47. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym. 48. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni. 49. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1. 50. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych. 51. Możliwość skanowania SSL dla połączeń RDP. 52. Program testowy – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Programy wczesnego dostępu powinny umożliwiać testowanie najnowszych funkcji oprogramowania których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.

	53. Oprogramowanie musi umożliwiać przystąpienie do programu testowego dostępnego dla systemów Linux i Windows który umożliwia przegląd konfiguracji punktów końcowych w czasie rzeczywistym poprzez tworzenie zapytań pod kątem wykrywania: a) historia powłoki b) wczytywanie bibliotek .dll z podejrzanej lokalizacji c) Sesje logowania z użyciem jawnych danych uwierzytelniających d) Elementy startowe Windows e) Arp cache f) Ip forwarding g) Pobieranie listy wszystkie otwarte pliki dla każdego procesu w systemie docelowym. h) Lista zamontowanych nośników i) Filtry ip tables j) Połączenia TLS które używają certyfikatów self-signed k) Używane rozszerzenia w przeglądarce Chrome l) Używane rozszerzenia w przeglądarce Firefox m) Używane rozsrzerzenia w przeglądarce Safari n) Źródła apt w systemach Linux o) Wyświelanie zainstalowanych pakietów DEB p) Wyświetlanie zainstalowanych pakietów RPM q) Pakiety Python zainstalowane w systemie r) Lista zainstalowanych użytkowników którzy łączyli się z publicznych adresów IP s) Lista użytkowników którzy zostali utworzeni w ciągu ostatnich 30 dni(Linux) t) Wykrywanie czy aplikacje zdalnego dostępu są zainstalowane w systemie MacOS u) Wykrywanie czy Kontrola Kont Użytkowników(UAC) jest wyłączona v) Wykrywanie czy SecureBoot jest włączony w) Lista zapamiętanych połączeń bezprzewodowych x) Wykrywa, czy zmienił się domyślny folder startowy użytkownika y) Wykrywa, czy zmienił się domyślny folder startowy maszyny 54. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. 55. Oprogramowanie musi umożliwiać przypisywanie znaczników ręcznie lub automatycznie 56. Oprogramowanie musi umożliwiać filtrowanie punktów końcowych na podstawie wybranych znaczników, musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.

	57. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows
4.	Wykupione wsparcie i licencja 60 m-cy

2.11 TABLET – 18 SZT.

Lp.	Minimalne wymagania
1.	Przekątna ekranu Min. 10,4''
2.	Rozdzielczość min. 2000 x 1200
3.	Rodzaj matrycy IPS
4.	System operacyjny Android 11 lub równoważny. System równoważny musi spełniać poniższe wymagania: • Zapewnia wielozadaniowość, wielowątkowość, pamięć wirtualną i możliwość zarządzania pamięcią. • Umożliwia uruchomienie dwóch aplikacji obok siebie na jednym ekranie. • Zapewnia szybkie przełączenie pomiędzy aplikacjami poprzez dwukrotne kliknięcie. • Umożliwia spersonalizowanie ustawień według preferencji użytkownika. • Możliwość zmiany kolejności kafelków. • Możliwość bezpośredniej odpowiedzi na powiadomienie, możliwość grupowania powiadomień. • Możliwość indywidulanego ustawienia ograniczenia ilości danych zużywanych przez urządzenie. • Personalizacja rozmiaru wyświetlacza. • Pobieranie aktualizacji w tle bez konieczności wyłączenia urządzenia. • Wbudowany menadżer pamięci. • Możliwość zapisywania danych w chmurze. • Możliwość instalacji innych aplikacji z dedykowanego sklepu. • Posiada aktualne wsparcie producenta. • Posiada dostęp do aktualizacji bezpieczeństwa.
5.	Taktowanie procesora 1,8 GHz
6.	Procesor klasy x64, min. 8-rdzeniowy, zaprojektowany do pracy z urządzeniami przenośnymi,

	na poziomie wydajności liczonej w punktach min. 2500 w teście PassMark CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/ - stan nie wcześniej niż dzień ogłoszenia postępowania. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. **Do oferty załączyć wydruk ze strony potwierdzający osiągany wynik.**
7.	Zainstalowana pamięć RAM min. 8 GB
8.	Pamięć wewnętrzna 128 GB
9.	Typ kart pamięci microSD
10.	Rozdzielczość Aparat - Przód 5 Mpix
11.	Rozdzielczość Aparat - Tył 8 Mpix
12.	Komunikacja • Wi-Fi (802.11a/b/g/n/ac) • Bluetooth 5.0 • LTE (4G)
13.	Modem WWAN (3G) / LTE (4G), wbudowany
14.	Funkcja telefonu komórkowego
15.	GPS
16.	Gniazda we/wy - 1 x 3,5 mm minijack, - 1 x USB (Type C)
17.	Pojemność baterii min. 6000 mAh

2.12 DOPOSAŻENIE ERADA – KAMERA – 1 SZT.

Lp.	Minimalne wymagania
1.	Przetwornik obrazu 5 MPX, matryca CMOS, 1/2.7”, OmniVision
2.	Liczba efektywnych pikseli: 2688 (H) x 1944 (V)

3.	Czułość: 0.007 lx/F1.4 - tryb kolorowy, 0 lx (IR wł.) - tryb czarno-biały
4.	Elektroniczna migawka automatyczna/manualna: 1/3 s ~ 1/100000 s
5.	Wydłużona migawka (DSS): do 1/3 s
6.	Szeroki zakres dynamiki (WDR): tak (podwójne skanowanie przetwornika), 120dB
7.	Cyfrowa redukcja szumu (DNR) 2D, 3D
8.	Funkcja Defog (F-DNR)
9.	Redukcja efektu oślepienia kamery (HLC)
10.	Kompensacja tylnego światła (BLC)
11.	Redukcja migotania obrazu (Antiflicker)
12.	Typ obiektywu motor-zoom z automatyczną przysłoną, f=2.8 ~ 12 mm/F1.4
13.	Auto-focus po zmianie krotności zoomu, przy przełączaniu pomiędzy trybami dzień/noc, wyzwalany ręcznie
14.	DZIEŃ/NOC Rodzaj przełączania: mechaniczny filtr podczerwieni
15.	Tryb przełączania: automatyczny
16.	Rozdzielczość strumienia wideo 2592 x 1944, 1920 x 1080
17.	Prędkość przetwarzania: 30 kl/s dla 2592 x 1944, 60 kl/s dla 1920 x 1080 (Full HD) i niższych rozdzielczości
18.	Tryb wielostrumieniowy 3 strumienie
19.	Kompresja wideo/audio: H.264, H.264+, H.264 Smart, H.265, H.265+, H.265 Smart, MJPEG / G.711
20.	Liczba jednoczesnych połączeń maks. 10
21.	Przepustowość łącznie 60 Mb/s

22.	Obsługiwane protokoły sieciowe HTTP, TCP/IP, IPv4, IPv4/v6, UDP, HTTPS, Multicast, FTP, DHCP, DDNS, NTP, RTSP, SNMP, QoS/DSCP, IEEE 802.1X, PPPoE, SMTP, RTCP, ICMP, Unicast, SSL/TLS
23.	Wsparcie protokołu ONVIF Profile S/G/T
24.	Detekcja ruchu
25.	Obszar obserwacji (ROI) 8
26.	Analiza obrazu sabotaż, przekroczenie linii, wkroczenie do strefy, wyjście ze strefy, zliczanie obiektów, detekcja twarzy, detekcja osób, detekcja osób nienoszących maski, zliczanie przekroczeń linii, zmiana sceny, utrata ostrości, zmiana kolorystyki, rozróżnianie obiektów, zliczanie osób, detekcja pojazdów, zliczanie pojazdów
27.	Obróbka obrazu: obrót obrazu o 180°, wyostrzanie, odbicie lustrzane, tryb korytarzowy, przerzucenie obrazu w pionie, przerzucenie obrazu w poziomie, korekcja efektu dystorsji obiektywu
28.	Reakcja na zdarzenia alarmowe e-mail, e-mail z załącznikiem, zapis na FTP, zapis na kartę SD
29.	OŚWIETLACZ IR Liczba LED 3 Zasięg 50 m Smart IRtak (wsparcie programowe)
30.	INTERFEJSY Wejścia/wyjścia audio 1 x Jack (3.5 mm)/- wbudowany mikrofon Interfejs sieciowy 1 x Ethernet - złącze RJ-45, 10/100 Mbit/s Gniazdo kart pamięci microSD - pojemność do 256GB
31.	Klasa szczelności IP 67
32.	Obudowa wandaloodporna stopień ochrony IK10 aluminiowa
33.	Zasilacz 12 VDC, PoE (IEEE 802.3af, Klasa 3)