Załącznik nr 1
do Zapytania ofertowego nr BZ.0404.1.2024.KA

Specyfikacja przedmiotu zamówienia

1. Przedmiotem zamówienia jest dostarczenie, zainstalowanie i pełne wdrożenie urządzeń IT zgodnych z opisem poniżej. Zamówienie jest podzielone na etapy. Dopuszczalne jest zgłoszenie się do konkretnego etapu, nie całości zamówienia.

2. Wymagania przedmiotu zamówienia:
   a) Dostawa na koszt i ryzyko Oferenta urządzeń IT do miejsca wskazanego przez Zamawiającego w dni robocze w godzinach 08:00-16:00, z wyłączeniem dni ustawowo wolnych od pracy.
   b) Oferent udzieli dodatkowo, nieodpłatnie gwarancji (poza gwarancją producenta) na okres 3 lat od dnia podpisania protokołu odbioru w ramach, której usunie wszelkie awarie, usterki, i wady urządzeń IT wraz z oprogramowaniami. Gwarancja nie obejmuje licencji na backup. W ramach uprawnień z gwarancji Oferent zapewni:
      - punkt kontaktowy (telefoniczny, e-mail oraz serwis internetowy producenta) do zgłaszania w języku polskim nieprawidłowości w działaniu urządzeń IT wraz z oprogramowaniami dostarczonego w ramach Umowy,
      - obsługę w zakresie udzielenia konsultacji i pomocy technicznej dotyczącej działania urządzeń IT wraz z oprogramowaniami dostarczonymi w ramach Umowy pod numerem telefonu ..... lub adresem e-mail ..... wskazanymi w umowie, w godzinach pracy Zamawiającego tj. w dni robocze od godziny 8:00 do godziny 16:00 w języku polskim,
      - naprawę lub wymianę urządzeń IT na nowy w ciągu 1-5 dni roboczych od zgłoszenia wady.

      Oferent, na czas trwania naprawy urządzeń IT, jest zobowiązany do dostarczenia i uruchomienia Sprzętu zastępczego, wolnego od nieprawidłowości, a ponadto zapewnienia sprawnego działania oprogramowania umożliwiającego jego wykorzystanie w zakresie funkcji opisanych w dokumentacji urządzeń IT.

Sąd Rejonowy dla Łodzi-Śródmieścia, XX Wydział Krajowego Rejestru Sądowego, numer KRS: 0000014128 | NIP: 725-14-86-825 | REGON: 471537330
Rachunek bankowy: PKO BP S.A. I o/Łódź 58 1020 3352 0000 1102 0011 0445 | Kapitał zakładowy 24.927.000 PLN | Kapitał wpłacony 24.927.000 PLN

3. Etapy zamówienia:
   a) Dostarczenie produktów zgodnym ze specyfikacją poniżej wraz z całym potrzebym osprzętem w terminie zgodnym ze złożoną ofertą.

1. Szafa rack:

	Wymagania techniczne
1	Wysokość – 42U (szer./gł. 800x1000).
2	Typ: Wolnostojąca.
3	Panel podłogowy: 4 kółka z hamulcem + regulowane nóżki.
4	Ładowność: do 799 KG.
5	Stopień ochrony: IP20.
6	Góra z półką na wentylatory: w zestawie 4 wentylatory 230 V w górnej pokrywie.
7	Typ drzwi: Przód - Perforowane, Tył – Perforowane (drzwi jednoskrzydłowe).
8	Kolor czarny (RAL9004).
9	Kąt otwarcia drzwi przednich: 215°.
10	Ilość pionowych szyn: 4.
11	Szczegóły uziemienia: drzwi przedmie i tylne, rama.
12	W zestawie z szafą: Kabel uziemiający, Pionowy organizer kabli x2, Zamek przedni, Zamek tylny, Zamki boczne.
13	Standard: ANSI/EIA RS-310-D, DIN 41491/PART 1, DIN 41494/PART 7, ETSI, IEC297-2:1982.
14	Wymaga się dostarczenia szafy złożonej gotowej do użytkowania.
15	Gwarancja: minimum 12 miesięcy.

2. Przełączniki sieciowe w ilości 2 sztuk:

	Wymagania techniczne
	1. Minimum 24 porty 1/10-gigabitowe SFP+ umieszczone z przodu obudowy. 2. Minimum 4 porty 1/10/25/50-gigabitowe SFP56 umieszczone z przodu obudowy. 3. Przepustowość: minimum 880 Gb/s (pełna prędkość, tzw. Wire-speed, na wszystkich portach przełącznika). 4. Wydajność: minimum 650 Mp/s. 5. Bufor pakietów: minimum 7.5 MB. 6. Minimum 8GB pamięci operacyjnej. 7. Minimum 30GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash). 8. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych. 9. Dedykowany port konsoli USB. 10. Port USB 2.0 (niezależny od portu konsoli USB). 11. Interfejs Bluetooth (dopuszcza się rozwiązanie w postaci adaptera Bluetooth, podłączanego do portu USB przełącznika, przy czym adapter musi pochodzić od tego samego producenta co przełącznik).

	12. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 10 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. 13. Łączenie w stos z wykorzystaniem portów 10Gb, 25Gb, 50Gb i agregowanych portów 10Gb, 25Gb i 50Gb (w celu zwiększenia przepustowości w stosie). Musi być możliwe stworzenie stosu z urządzeń oddalonych od siebie o co najmniej 1000 metrów. 14. Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie. 15. Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia. 16. Modularne, redundantne wentylatory, podzielone na co najmniej dwa niezależne moduły. Moduły wentylatorów musi mieć możliwość wymiany „na gorąco" (na działającym urządzeniu). 17. Wielkość tablicy routingu: minimum 60000 wpisów Ipv4, 60000 wpisów Ipv6. 18. Tablica routingu multicast o pojemności co najmniej 8000 wpisów dla Ipv4 oraz co najmniej 8000 wpisów dla Ipv6. 19. Tablica adresów MAC o wielkości minimum 32000 pozycji. 20. Obsługa Jumbo Frames o wielkości co najmniej 9198B. 21. Obsługa sFlow lub Netflow. 22. Obsługa skryptów w języku Python. 23. Obsługa REST API. 24. Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty. 25. Obsługa RMON (minimum grupy 1,2,3 i 9). 26. Obsługa 4000 jednoczesnych sieci VLAN 802.1Q. 27. Obsługa standardu 802.1v. 28. Obsługa protokołu MVRP. 29. Obsługa Ethernet Ring Protection Switching (ERPS). 30. Wsparcie dla VXLAN. 31. Obsługa Microsoft Network Load Balancer (NLB). 32. Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne. 33. Obsługa Rapid Spanning Tree (802.1w) I Multiple Spanning Tree (802.1s). 34. Obsługa Secure FTP lub SCP 35. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP). 36. Obsługa SNTPv4 lub NTP.

	37. Wsparcie dla Ipv6 (Ipv6 host, dual stack, MLD snooping, ND snooping). 38. Obsługa protokołów rutingu: ruting statyczny, RIPv2, RIPng, OSPF, OSPFv3, BGP, MP-BGP. 39. Obsługa ruchu multicast: IGMPv1/v2/v3, PIM-SM, PIM-DM, MSDP. 40. Obsługa VRRP. 41. Obsługa ECMP. 42. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) I LLDP Media Endpoint Discovery (LLDP-MED). 43. Mechanizmy związane z zapewnieniem jakości usług w sieci: priorytetyzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla minimum 8 kolejek sprzętowych, rate-limiting. 44. Obsługa uwierzytelniania użytkowników zgodna z 802.1x. 45. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS. 46. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW. 47. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie. 48. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+. 49. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+. 50. Wbudowany serwer DHCP. 51. Obsługa funkcji User Datagram Protocol (UDP) helper. 52. Obsługa blokowania nieautoryzowanych serwerów DHCP. 53. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego. 54. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection). 55. Obsługa list kontroli dostępu (ACL) bazujących na porcie oraz na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP. Musi być możliwe utworzenie minimum 20000 wpisów ACL typu ingress opartych o Ipv4 oraz minimum 20000 wpisów ACL typu ingress opartych o MAC. 56. Zakres pracy od 0 do 45°C. 57. Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 40 cm. 58. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania. 59. Wszystkie wymagane funkcje muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji o ile nie wyspecyfikowano inaczej. 60. Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy

	przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do pomocy technicznej oraz poprawek i aktualizacji oprogramowania przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. 61. Wymagania dodatkowe: - Zamawiający może zażądać przed dostawą przeprowadzenia testów wybranych funkcji sprzętu i oprogramowania wymaganych w niemniejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłuższym niż 2 tygodnie od chwili zażądania przez Zamawiającego ich przeprowadzenia. Nieprzystąpienie do testów lub nieskuteczne ich przeprowadzenie (brak potwierdzenia przez Zamawiającego, że testy zostały zakończone pomyślnie) skutkować będzie odrzuceniem oferty. - Sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim. - Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych. - Urządzenie musi być fabrycznie nowe. Przed dostawą sprzęt musi być zarejestrowany przez producenta, bezpośrednio na Zamawiającego jako jedynego użytkownika po opuszczeniu fabryki. Jeśli producent nie prowadzi rejestracji sprzętu, to wymaga się deklaracji producenta, iż sprzęt jest fabrycznie nowy. - Zamawiający może zażądać przed dostawą dokumentu zawierającego numer seryjny dostarczanego sprzętu w celu weryfikacji spełnienia warunków gwarancyjnych. Zamawiający sprawdzi spełnienie powyższych warunków w polskim biurze producenta na podstawie numeru seryjnego urządzenia – w przypadku niezgodności deklaracji Wykonawcy z opinią producenta Zamawiający odmówi odbioru przedmiotu zamówienia, jako niezgodnego ze specyfikacją istotnych warunków zamówienia.

3. Kabel DAC

	Wymagania techniczne
1	Kabel 10GbE DAC SFP+ o długości co najmniej 3 metry – 2 sztuki. Kable DAC SFP+ muszą być w pełni kompatybilne z przełącznikami opisanymi w tym dokumencie. W szczególności

	muszą być wskazane jako dedykowane w oficjalnych kartach katalogowych przełącznika oraz muszą być serwisowane przez serwis producenta przełącznika. Min. 12 miesięcy gwarancji.

4. Kabel DAC

	Wymagania techniczne
1	Kabel 10GbE DAC SFP+ o długości co najmniej 1 metr SFP+ – 2 sztuki i 2 metry SFP+ - 2 sztuki. Kable muszą być w pełni kompatybilne z przełącznikami opisanymi w tym dokumencie. W szczególności muszą być wskazane jako dedykowane w oficjalnych kartach katalogowych przełącznika oraz muszą być serwisowane przez serwis producenta przełącznika. Min. 12 miesięcy gwarancji.

b) Dostarczenie produktów zgodnym ze specyfikacją poniżej wraz z całym potrzebym osprzętem w terminie zgodnym ze złożoną ofertą.

1. Firewall w klastrze dwóch tych samych urządzeń

Wymagania Ogólne

System bezpieczeństwa musi posiadać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall ma zapewnić pracę w jednym z trzech trybów: Routera
z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System ma umożliwić budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu.

System ma wspierać protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

1	Redundancja, monitoring i wykrywanie awarii
1.1	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
1.2	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
1.3	Monitoring stanu realizowanych połączeń VPN.
1.4	System ma umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
2	Interfejsy, Dysk, Zasilanie
2.1	System realizujący funkcję Firewall ma dysponować co najmniej poniższą liczbą i rodzajem interfejsów:

	• 18 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 4 gniazdami SFP+ 10 Gbps.
2.2	System Firewall ma posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2.3	System Firewall ma pozwalać na skonfigurowanie co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
2.4	System ma być wyposażony w zasilanie 2xAC.
3	Parametry wydajnościowe:
3.1	W zakresie Firewall'a ma zapewnić obsługę nie mniej niż 3 mln jednoczesnych połączeń oraz 260 tys. nowych połączeń na sekundę.
3.2	Przepustowość Stateful Firewall: nie mniej niż 26 Gbps dla pakietów 512 B.
3.3	Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 12.6 Gbps.
3.4	Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 12 Gbps.
3.5	Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 4.8 Gbps.
3.6	Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps.
3.7	Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3.9 Gbps.
4	Funkcje Systemu Bezpieczeństwa:
4.1	W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
5	Parametry wydajnościowe:
5.1	Polityka Firewall ma uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
5.2	System ma realizować translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu.

	• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
5.3	W ramach systemu ma istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
5.4	Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5.5	Polityka firewall ma umożliwiać filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
5.6	Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5.7	Element systemu realizujący funkcję Firewall ma integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
6	Połączenia VPN
6.1	System ma umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site.
6.2	System ma umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi posiadać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
7	Routing i obsługa łączy WAN
7.1	W zakresie routingu rozwiązanie ma zapewniać obsługę: 1. Routingu statycznego.

	2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
8	Funkcje SD-WAN
8.1	System ma umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
8.2	SD-WAN ma wspierać zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
9	Zarządzanie pasmem
9.1	System Firewall ma umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
9.2	System ma umożliwiać określanie pasma dla poszczególnych aplikacji.
9.3	System ma pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
9.4	System ma zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
10	Ochrona przed malware
10.1	Silnik antywirusowy ma umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
10.2	Silnik antywirusowy ma zapewnić skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
10.3	System ma umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
10.4	System ma umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
10.5	System ma dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
10.6	Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
10.7	System ma zapewnić współpracę z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
10.8	System ma zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
10.9	Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10.10	Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
11	Ochrona przed atakami
11.1	Ochrona IPS ma opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
11.2	System ma chronić przed atakami na aplikacje pracujące na niestandardowych portach.

11.3	Baza sygnatur ataków ma zawierać minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
11.4	Administrator systemu ma zapewnić możliwość definiowania własnych wyjątków oraz własnych sygnatur.
11.5	System ma zapewnić wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
11.6	Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
11.7	Możliwość kontrolowania długości nagłówka, ilości parametrów URL dla protokołu http.
11.8	Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
11.9	Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
12	Kontrola aplikacji
12.1	Funkcja Kontroli Aplikacji ma umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
12.2	Baza Kontroli Aplikacji ma zawierać minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora
12.3	Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
12.4	Baza sygnatur ma zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
12.5	Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
12.6	Z możliwością blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
12.7	System ma umożliwiać określenie dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
13	Kontrola WWW
13.1	Moduł kontroli WWW ma korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
13.2	W ramach filtra WWW muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
13.3	Filtr WWW ma dostarczać kategorii stron zabronionych prawem np.: Hazard.
13.4	Administrator ma mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
13.5	Filtr WWW ma umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
13.6	Filtr WWW ma umożliwiać wykonanie akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
13.7	Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo
13.8	Administrator ma mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
13.9	System ma pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji
14	Uwierzytelnianie użytkowników w ramach sesji
14.1	System Firewall ma umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

	• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
14.2	System ma umożliwiać zastosowanie w tym procesie uwierzytelniania dwuskładnikowego.
14.3	System ma umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
14.4	Uwierzytelnianie ma następować w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
15	Zarządzanie
15.1	Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
15.2	Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania ma być realizowana z wykorzystaniem szyfrowanych protokołów.
15.3	Z możliwością włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
15.4	System ma współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
15.5	System ma umożliwiać zarządzanie przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
15.6	Element systemu pełniący funkcję Firewall ma posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
15.7	Element systemu realizujący funkcję Firewall ma umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
15.8	Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
15.9	Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
16	Logowanie
16.1	Elementy systemu bezpieczeństwa zrealizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
16.2	W ramach logowania element systemu pełniący funkcję Firewall ma zapewniać przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
16.3	Logowanie ma obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
16.4	Możliwość włączenia logowania per reguła w polityce firewall.
16.5	System ma zapewniać możliwość logowania do serwera SYSLOG.
16.6	Przesyłanie SYSLOG do zewnętrznych systemów ma być umożliwione z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
17	Serwisy i licencje
17.1	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane bedą licencje:

	a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.
18	Gwarancja oraz wsparcie
18.1	System ma być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

2. Centralny system logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych

Wymagania Ogólne

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej

w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure Google Cloud (GCP)

1	Interfejsy, Dysk:
1.1	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.
2	Parametry wydajnościowe:
2.1	System musi być w stanie przyjmować minimum 5 GB logów na dzień.
2.2	Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.
3	Logowanie
3.1	Podgląd logowanych zdarzeń w czasie rzeczywistym
3.2	Możliwość przeglądania logów historycznych z funkcją filtrowania.
3.3	System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: a. Listę najczęściej wykrywanych ataków. b. Listę najbardziej aktywnych użytkowników. c. Listę najczęściej wykorzystywanych aplikacji. d. Listę najczęściej odwiedzanych stron www. e. Listę krajów, do których nawiązywane są połączenia.

	f. Listę najczęściej wykorzystywanych polityk Firewall. g. Informacje o realizowanych połączeniach IPSec.
3.4	Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
3.5	Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514
3.6	System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
4	Raportowanie
4.1	Generowanie raportów co najmniej w formatach: PDF, CSV.
4.2	Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
4.3	Funkcję definiowania własnych raportów
4.4	Możliwość spolszczenia raportów.
4.5	Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
5	Korelacja logów
5.1	Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
5.2	Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
5.3	Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
5.4	Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.
6	Zarządzanie
6.1	System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
6.2	System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
7	Serwisy i licencje
7.1	Wsparcie: System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

c) Dostarczenie produktów zgodnym ze specyfikacją poniżej wraz z całym potrzebym osprzętem w terminie zgodnym ze złożoną ofertą.

1. Macierz

1	Wymagania techniczne
1.1	Obudowa - gęstość upakowania : a. Możliwość zainstalowania w standardowej szafie RACK 19”. b. Urządzenie musi wykorzystywać półki dyskowe wysokiej gęstości upakowania - co najmniej 24 dyski na 2U wysokości dla dysków 2,5 cala oraz półki dyskowe zawierające co najmniej 12 dysków 3,5 cala na wysokości 2U.

	c. Urządzenie musi wykorzystywać półki dyskowe wysokiej gęstości umożliwiające upakowanie co najmniej 90 dysków na maksymalnej wysokości 5U. d. Wysokość oferowanego rozwiązania – maksymalnie 4 U.
1.2	Zarządzanie: a. Urządzenie musi umożliwiać zarządzanie za pomocą interfejsu Ethernet. b. Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. c. Funkcjonalność bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje.
1.3	Ilość portów: a. Wymagane jest nie mniej niż 4 porty 10Gb Ethernet Base-T oraz 8 portów 10Gb Ethernet SFP+ wyposażonych we wkładki SFP+ 10Gb SR.
1.4	Obsługa dysków: a. musi obsługiwać dyski SAS: - o prędkości obrotowej 10000 obr./min. i pojemności 2.4TB; - o prędkości obrotowej 7200 obr./min. i pojemnościach 8TB, 12TB, 16TB, 20TB; b. musi obsługiwać dyski SSD o pojemnościach 1.92 TB , 3.84 TB, 7.68 TB, 15.36 TB, 30.72 TB. c. musi wspierać obsługę co najmniej 420 dysków na parę kontrolerów z zastosowaniem dodatkowych półek. Macierz musi umożliwiać rozbudowę o pojedyncze dyski fizyczne i pojedyncze półki rozszerzeń. d. musi umożliwiać konfigurację, która w jednym rozwiązaniu łączyć będzie półki rozszerzeń na dyski 2,5" z półkami na dyski 3,5".
1.5	Pojemność dyskowa: Macierz dyskowa musi być wyposażona w minimum: 6 dysków SSD o pojemności 1.92TB 6 dysków NL-SAS 7200 obr./min. o pojemności 16TB Macierz musi posiadać co najmniej 18 wolnych slotów na dyski 2,5'' oraz 6 wolnych slotów na dyski 3,5'' pod rozbudowę w przyszłości.
1.6	Macierz musi zapewnić możliwość wymiany uszkodzonych dysków podczas pracy systemu (Hot-Swap). Macierz musi umożliwiać stworzenie konfiguracji odpornej na awarię dwóch dysków. Przestrzeń zapasowa powinna być realizowana za pomocą przestrzeni zapasowej rozmieszczonej na wszystkich dyskach w ramach grupy RAID lub w formie dysku nadmiarowego.
1.7	Obsługa pamięci Cache: a. Macierz musi być wyposażona w minimum 64GB pamięci Cache. Macierz musi umożliwiać rozbudowę pamięci cache do 128GB w ramach klastra macierzy zarządzanego z jednego interfejsu GUI, CLI.
1.8	Wsparcie dla systemów operacyjnych: Macierz musi wspierać następujące systemy operacyjne i wirtualizatory: MS Windows Server 2016,2019/2022, VMware vSphere 7.x/8.x, Red Hat Enterprise Linux 8.x/9.x
2	Dodatkowe wymagania i funkcjonalności
2.1	Funkcje niezawodnościowe: a. Wszystkie krytyczne komponenty urządzenia takie jak: kontrolery dyskowe, pamięć cache, zasilacze i wentylatory muszą być zdublowane tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. b. Komponenty te muszą być wymienialne w trakcie pracy macierzy. c. Urządzenie musi cechować brak pojedynczego punktu awarii. d. Wsparcie dla zasilania z dwóch niezależnych źródeł prądu poprzez nadmiarowe zasilacze typu Hot-Swap.

	e. Wentylatory typu Hot-Swap. f. Wbudowane co najmniej dwa kontrolery RAID. g. Urządzenie musi posiadać pamięć typu Flash dla zapisu danych z pamięci cache na wypadek zaniku zasilania oraz system podtrzymania zasilania pozwalający na zapis danych z cache do pamięci typu Flash.
2.2	Funkcjonalności: a. Musi istnieć funkcjonalność Cache dla procesu odczytu. b. Musi istnieć funkcjonalność Mirrored Cache dla procesu zapisu. c. Możliwość wyłączenia cache dla poszczególnych wolumenów. d. Funkcjonalność partycjonowania pamięci cache. e. Funkcjonalność separacji przestrzeni dyskowych pomiędzy różnymi podłączonymi hostami. f. Funkcjonalność dynamicznego zwiększania i zmniejszania rozmiaru wolumenów. g. Funkcjonalność zarządzania ilością operacji wejścia / wyjścia wykonywanych na danym wolumenie – zarządzanie musi być możliwe zarówno poprzez określenie ilości operacji I/O na sekundę jak również przepustowości określonej w MB/s. h. Urządzenie musi obsługiwać funkcjonalność ochrony przed skasowaniem lub odmapowaniem od hosta woluminu dyskowego, do którego były przesłane operacje wejścia/wyjścia w określonym przez użytkownika czasie. i. Dostępne sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu dla podłączanych systemów operacyjnych (jeżeli jest wymagana licencja, należy dostarczyć licencje na całość oferowanych zasobów).
2.3	Obsługa wirtualnych dysków logicznych: a. Minimalna ilość wspieranych wirtualnych dysków logicznych (LUN) dla całej (globalnej) puli dyskowej musi wynosić co najmniej 2000. Funkcjonalność LUN Masking i LUN Mapping. b. Urządzenie musi umożliwiać stworzenie mirrorowanych LUN pomiędzy różnymi typami dysków, dla których awaria jednej kopii lustra musi być niezauważalna dla systemu hosta.
2.4	Funkcjonalność thin provisioning: Urządzenie musi obsługiwać funkcjonalność thin provisioning dla wszystkich wolumenów. Musi istnieć możliwość wyłączenia tej funkcjonalności dla wybranych wolumenów. Należy dostarczyć licencję umożliwiającą korzystanie z funkcji thin provisioning na całą oferowaną pojemność urządzenia.
2.5	Kopie migawkowe: Macierz musi umożliwiać tworzenie wg ustalonego harmonogramu odpornych na zagrożenia cybernetyczne kopii wolumenów, których nie można zmienić ani usunąć w wyniku błędów użytkownika, złośliwych działań lub ataków oprogramowania ransomware.
2.6	Migracja wolumenów logicznych: Urządzenie musi mieć możliwość wykonania migracji wolumenów logicznych pomiędzy różnymi typami dysków wewnątrz macierzy bez zatrzymywania aplikacji korzystającej z tych wolumenów. Wymaga się, aby zasoby źródłowe podlegające migracji oraz zasoby do których są migrowane mogły być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (SAS, SSD, SATA).
2.7	Replikacja macierzy : Urządzenie musi posiadać funkcjonalność replikacji danych przy użyciu synchronicznych oraz asynchronicznych transmisji danych przez łącza komunikacyjne IP oraz FC lub FCoE. Macierz musi przechowywać w pełni zsynchronizowaną kopię w odległości do 300km. Przy znacznie większej odległości, do 8000km, replikacje mogą działać asynchronicznie. Oba rodzaje replikacji muszą wspierać program Vmware Site Recovery Manager do odzyskiwania danych po awarii. Jeśli na obsługę powyższej funkcjonalności wymagana jest dodatkowa licencja, jest ona wymagana w tym postępowaniu.

2.8	Wirtualizacja zasobów: Macierz musi mieć możliwość wirtualizacji zasobów znajdujących się na innych niż oferowana macierz dyskowa na potrzeby migracji danych. Migracja musi się odbyć w trybie bezprzerwowym.
2.9	Kompresja i deduplikacja danych: Macierz musi mieć możliwość kompresji i deduplikacji danych. Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową.
2.10	Macierz musi mieć funkcjonalność wykonywania pełnej kopii lokalnych wolumenów logicznych z wykorzystaniem jedynie kontrolerów macierzy. Licencja na wykonywanie kopii lokalnego wolumenu powinna umożliwiać utworzenie co najmniej 4000 kopii.
2.11	Macierz musi mieć możliwość uruchomienia funkcjonalności szyfrowania danych na poziomie kontrolerów macierzowych. Jeśli na obsługę powyższej funkcjonalności wymagana jest dodatkowa licencja, nie jest ona wymagana w tym postępowaniu.
2.12	Macierz musi mieć możliwość dodawania kolejnych półek dyskowych oraz dysków bez przerywania pracy macierzy, dla dowolnej konfiguracji macierzy.
2.13	Macierz musi mieć możliwość aktualizacji oprogramowania macierzy (firmware) w trybie online.
2.14	Macierz musi umożliwiać tworzenie wolumenów o pojemności nie mniejszej niż 250 TB.
2.15	Do macierzy należy dołączyć przewody zasilające oraz 4 przewody światłowodowe o długości 5m.
2.16	Macierz musi posiadać funkcjonalność optymalizacji wykorzystania dysków SSD/Flash poprzez automatyczną identyfikację najbardziej obciążonych fragmentów wolumenów w zarządzanych zasobach dyskowych oraz ich automatyczną migrację na dyski SSD/Flash. Macierz musi również automatycznie rozpoznawać obciążenie fragmentów wolumenów na dyskach SSD/Flash i automatycznie migrować z dysków SSD/Flash nieobciążone fragmenty wolumenów. Macierz musi posiadać możliwość wykorzystania mechanizmu optymalizacji umiejscowienia danych pomiędzy przynajmniej 3 rodzajami dysków – SSD/Flash, Enterprise (SAS 10k) oraz NL-SAS/SATA, jak również przy wykorzystaniu dwóch dowolnych z wyżej wymienionych typów. Opisany powyżej proces optymalizacji musi posiadać funkcję włączenia/wyłączenia na poziomie pojedynczego wolumenu. Jeśli na obsługę powyższej funkcjonalności wymagana jest dodatkowa licencja, jest ona wymagana w tym postępowaniu.
2.17	Zaoferowana macierz musi posiadać możliwość implementacji klastra geograficznego. W ramach architektury klastra geograficznego musi być wspierane bezprzerwowe migrowanie maszyn wirtualnych pomiędzy ośrodkami. W przypadku awarii jednego z ośrodków nastąpi bezprzerwowe przełączenie do lokalizacji zapasowej. Powyższa funkcjonalność musi być realizowana niezależnie od systemu operacyjnego na poziomie przełączania ścieżek do urządzenia logicznego.
3	Inne
3.1	Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu.
3.2	Oferowane produkty (urządzenia, sprzęty) w przedmiotowym postępowaniu o udzielenie zamówienia publicznego muszą spełniać wymagania norm CE, tj. muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE.
3.3	Wszystkie oferowane urządzenia muszą być fabrycznie nowe.
3.4	Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
3.5	Urządzenie musi współpracować z siecią energetyczną o parametrach w przedziale 200V-230V, 50 Hz.

3.6	Macierz dyskowa musi być objęta gwarancją świadczoną w reżimie 9x5 przez okres 36 miesięcy z reakcją maksymalnie w następnym dniu roboczym od momentu zgłoszenia usterki. Ze względu na 36 miesięczny okres Zamawiający wymaga, aby usługi serwisowe świadczone były wyłącznie przez producenta oferowanego sprzętu, nie dopuszcza się świadczenia serwisu przez autoryzowanych partnerów producenta.
3.7	Zgłoszenia usterek muszą być akceptowane przez producenta zarówno drogą email jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.). Linia telefoniczna musi być czynna 24 godziny na dobę, 7 dni w tygodniu również w dni świąteczne.
3.8	Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia przez cały okres obowiązywania gwarancji.

2. Serwer:

1	Wymagania techniczne
2	Obudowa ● Typu RACK, wysokość 2U; ● Szyny umożliwiające wysunięcie serwera z szafy stelażowej; ● Możliwość zainstalowania 10 dysków twardych hot plug 3,5″; ● Możliwość zainstalowania fizycznego zabezpieczenia (np. na klucz lub elektrozamek) uniemożliwiającego fizyczny dostęp do dysków twardych; ● Zainstalowane 4 szt. dysków SATA 2TB Hot-Plug skonfigurowane w RAID podpięte do sprzętowego kontrolera;

3	Płyta główna
	● Dwuprocesorowa;
	● Wyprodukowana i zaprojektowana przez producenta serwera;
	● Możliwość instalacji procesorów 38-rdzeniowych;
	● Moduł TPM 2.0;
	● 7 złącz PCI Express generacji 4 w tym:
	  ● 4 fizyczne złącza o prędkości x16;
	  ● 3 fizyczne złącza o prędkości x8;
	● 32 gniazda pamięci RAM;
	● Obsługa minimum 4 TB pamięci RAM DDR4;
	● Obsługa 10 TB pamięci operacyjnej w konfiguracji RAM DDR4 + pamięć nieulotna;
	● Wsparcie dla technologii:
	  ● Memory Scrubbing;
	  ● SDDC;
	  ● ECC;
	  ● Memory Mirroring;
	  ● ADDDC;
	● Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci);

	● Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug.
4	Procesory a. Procesor 8-rdzeniowy, taktowanie bazowe 2,8 GHz, architektura x86_64; b. osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 152 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html.
5	Pamięć RAM • 128 GB pamięci RAM; • DDR4 Registered 3200Mhz.
6	Kontrolery LAN Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express: ● 4x 1Gbit; ● Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe; Interfejsy LAN zainstalowane w slotach PCI-e: ● 2x 10Gbit SFP+ wraz z modułami SFP+ MMF LC.
7	Kontrolery I/O ● Kontroler SAS RAID dla dysków wewnętrznych, obsługujący poziomy RAID: 0,1,10,5,50;
8	Porty • Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; • 1 port USB 3.0 wewnętrzny; • 2 porty USB 3.0 dostępne z tyłu serwera; • 2 porty USB 3.0 na panelu przednim; • Możliwość instalacji portu serial, możliwość wykorzystania portu serial do zarządzania serwerem; • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.
9	Zasilanie, chłodzenie a. Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy nie mniejszej niż 900W; b. Redundantne wentylatory hotplug.
10	Zarządzanie ● Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii; ● informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: ● karty rozszerzeń zainstalowane w dowolnym slocie PCI Express; ● procesory CPU; ● pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM; ● wbudowany na płycie głównej nośnik pamięci M.2 SSD;

	● status karty zarządzającej serwera; ● wentylatory; ● bateria podtrzymująca ustawienia BIOS płyty głównej; ● zasilacze; ● system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym); ● Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: ● Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; ● Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; ● Dostęp poprzez przeglądarkę Web, SSH; ● Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; ● Zarządzanie alarmami (zdarzenia poprzez SNMP); ● Możliwość przejęcia konsoli tekstowej; ● Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); ● Obsługa serwerów proxy (autentykacja); ● Obsługa VLAN; ● Możliwość konfiguracji parametru Max. Transmission Unit (MTU); ● Wsparcie dla protokołu SSDP; ● Obsługa protokołów TLS 1.2, SSL v3; ● Obsługa protokołu LDAP; ● Integracja z HP SIM; ● Synchronizacja czasu poprzez protokół NTP; ● Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej; ● Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); ● Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB; ● Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;

	● Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.
11	Wspierane OS ● Microsoft Windows Server 2022, 2019, 2016; ● Microsoft Windows Storage Server Std 2016 ● VMWare vSphere 8.0; ● Hyper-V Server 2019.
12	Gwarancja ● 36 miesięcy gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej; ● Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; ● Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; ● Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniony w ofercie; ● Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie on-site z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki.
	Wymagania dodatkowe: ● Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta; ● Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; ● Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; ● W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; ● Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; ● Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %; Zgodność z normami: CB, RoHS, WEEE, oraz CE.
	3 sztuki Windows Server 2022 Standard 16 core lub równoważne o poniższych parametrach:

	3 x licencja na serwerowy system operacyjny min. 16 core. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy: 1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9) Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18) Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci,

centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.

20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
        iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c) Zdalna dystrybucja oprogramowania na stacje robocze.
    d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
    i. Dystrybucję certyfikatów poprzez http,
    ii. Konsolidację CA dla wielu lasów domeny,
    iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
    iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    f) Szyfrowanie plików i folderów.
    g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
    h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
    i) Serwis udostępniania stron WWW.
    j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
    k) Wsparcie dla algorytmów Suite B (RFC 4869),
    l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
    m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover

	z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych, iii. Obsługi 4-KB sektorów dysków, iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode). 26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

3. Licencja do backupu – 1 komplet:

1	Wymagania techniczne
2	• Ilość zaoferowanych licencji musi zapewnić wykonanie backupu min. 120 skrzynek pocztowych (Microsoft Office 365) posiadanych przez Zamawiającego. • Rozwiązanie musi wykonywać kopię zapasową danych Microsoft Exchange Online w ramach usługi Microsoft 365 oraz lokalnych instancji Microsoft Exchange. • Rozwiązanie musi wykonywać kopię zapasową danych Microsoft Sharepoint Online w ramach usługi Microsoft 365 oraz lokalnych instancji Microsoft Sharepoint. • Rozwiązanie musi wykonywać kopię zapasową danych Microsoft OneDrive for Business w ramach usługi Microsoft 365. • Rozwiązanie musi wykonywać kopię zapasową danych Microsoft Teams w ramach usługi Microsoft 365. • Rozwiązanie musi pozwalać na dodanie wielu subskrypcji Microsoft 365 oraz wielu lokalnych serwerów Exchange oraz Sharepoint. • Rozwiązanie nie może instalować żadnych agentów po stronie lokalnych instancji Exchange oraz Sharepoint. Wymaga się wykorzystania API wewnętrznych aplikacji. • Rozwiązanie nie może wymagać tworzenia dodatkowych elementów/agentów po stronie Microsoft 365. • Rozwiązanie nie może dodawać żadnych dodatkowych kont członkowskich do zabezpieczanych grup będących częścią zespołów MS Teams. • Rozwiązanie musi wspierać uwierzytelnianie wieloskładnikowe (MFA). • Rozwiązanie musi być licencjonowane per użytkownik. • Rozwiązanie musi być licencjonowane w modelu subskrypcyjnym.

	• Rozwiązanie musi posiadać skalowalną architekturę (serwer zarządzający, repozytorium). Nie dopuszcza się, aby komponenty systemu backupu były dodatkowo licencjonowane. • Rozwiązanie musi przechowywać dane w macierzystym formacie Microsoft Exchange. • Rozwiązanie musi pozwolić przechowywać dane na lokalnych zasobach oraz na zasobach obiektowych (Microsoft Azure Blob, Microsoft Azure Archive Blob, AWS S3 bucket, AWS S3 Glacier bucket oraz innych kompatybilnych z protokołem S3). • Rozwiązanie musi pozwalać na granularne odzyskiwanie dowolnych elementów Microsoft Exchange (skrzynka, mail, kontakt, wpis z kalendarza, element folderu „Permanently Deleted Items"). • Rozwiązanie musi pozwalać na granularne odzyskiwanie dowolnych elementów Microsoft Sharepoint. Opcja odtworzenia elementów, witryn. • Rozwiązanie musi pozwalać na granularne odzyskiwanie dowolnych elementów Microsoft OneDrive. Opcja odtworzenia plików, folderów lub całych kont OneDrive • Rozwiązanie musi pozwalać na granularne odzyskiwanie dowolnych elementów Microsoft Teams. Opcja odtworzenia całych zespołów, kanałów, zakładek, plików oraz konwersacji. • Rozwiązanie musi pozwalać na odzysk elementów do skrzynki w pakiecie Microsoft 365, lokalnej skrzynki Exchange, pliku oraz w formacie PST. • Rozwiązanie musi oferować webowy portal samoobsługowy pozwalający użytkownikom na granularne odzyskiwanie własnych obiektów z Exchange, Sharepoint oraz OneDrive. • Rozwiązanie musi pozwalać na delegowanie uprawnień odzyskiwania danych dla operatorów odtwarzania. • Rozwiązanie musi pozwalać na hybrydowe scenariusze backupu/odzysku (np. backup wykonany z lokalnej instancji Exchange, odzysk do Exchange Online w Microsoft 365). • Rozwiązanie musi pozwalać na granularne przeszukiwanie zabezpieczonych danych (eDiscovery) • Rozwiązanie musi mieć możliwość integracji z innymi rozwiązanymi poprzez PowerShell oraz RESTful API. • Rozwiązanie musi posiadać możliwość skonfigurowania audytu dla wybranych obiektów (np. dla skrzynki mailowej). Próba przeglądania, odtwarzania tych danych spowoduje wysłanie maila do audytora. • Licencja w formie subskrypcji na okres min. 12 miesięcy ze wsparciem 24/7.

4. Licencja do backupu – 1 komplet:

1	Wymagania techniczne
2	Wymagania ogólne: • Ilość zaoferowanych licencji musi zapewnić wykonanie backupu min. 6 maszyn wirtualnych na jednym serwerze fizycznym. • Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5. • Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej. • Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 6.7.x, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy. • Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. • Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej. • Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków. • Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji. • Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. • Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. • Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. • Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. • Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.

	• Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time). • Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu. • Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API. • Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji. • Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji. • Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania. • Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. • Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej. • Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora). • Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS) • Oprogramowanie musi posiadać integracje z systemami typu SIEM • Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji. • Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej. • Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. • Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru. • Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. • Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. • Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592). • Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son). • Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. • Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.

	• Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. • Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. • Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. • Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik. • Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding). • Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN). • Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. • Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna). • Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami. • Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre. • Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków. • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. • Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików. • Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. • Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell. • Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM. • Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. • Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.

	• Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. • Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. • Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. • Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. • Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN. • Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI. • Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2. • Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN. • Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna). • Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. • Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem. • Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. • Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware. • Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania. • Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków.

	• Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. • Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR. • Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego. • Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych. • Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE, Rocky Linux, AlmaLinux. • Rozwiązanie musi wspierać system operacyjny macOS. • Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix. • Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą). • Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster. • Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów. • Rozwiązanie musi wspierać backup podłączonych dysków USB. • Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym. • Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury). • Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone. • Rozwiązanie musi wspierać kontrolę pasma sieciowego. • Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych. • Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN. • Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft. • Rozwiązanie musi wspierać technologię BitLocker. • Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania. • Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych. • Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych. • Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu. • Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform • Rozwiązanie musi wspierać szyfrowanie.

	• Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne. • Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego. • Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej. • Rozwiązanie musi wspierać tworzenie wielu zadań backupowych. • Monitoring. • System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich. • System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie. • System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. • System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter. • System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn. • System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel. • System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk. • System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora. • System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów. • System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard). • System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna. • System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego. • System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta. • System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. • System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. • System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware. • System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.6.

	• System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie. • System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. • System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. • System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V. • System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF. • System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc. • System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach. • System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów. • System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych. • System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych. • System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury. • System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta. • System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. • System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'. • System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware. • System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots). • System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie • Licencja w formie subskrypcji na okres min. 12 miesięcy ze wsparciem 24/7.