Załącznik do zaprania ofertowego nr 1

Szczegółowy opis przedmiotu zamówienia
„Zakup sprzętu komputerowego oraz oprogramowania ”

Ogólne warunki realizacji zamówienia

1. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
2. Dostarczany sprzęt i oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.
3. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
4. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
5. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaże adresy WWW, pod którymi można je pobrać.
6. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji właściwemu dla danej części Zamawiającego lub przeniesienia na Odbiorcę niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

7.

Część I. Dostawa serwera, urządzeń pamięci masowej i oprogramowania

Zestawienie rzeczowo - ilościowe

Lp.	Przedmiot dostawy/usługi	Ilość
1.	Zakup serwera kopii zapasowych	1
2.	Zakup NAS z dyskami	1
3.	Zakup licencji oprogramowania backup	1

1.1 Zakup serwera kopii zapasowych

Obszar wymagań	**Wymagania minimalne**
Fabryczna konfiguracja serwera	Wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji muszą być zamontowane fabrycznie przez producenta serwera. W szczególności nie dopuszcza się modyfikacji fabrycznej konfiguracji przez wykonawcę czy montażu dodatkowych komponentów niepochodzących od producenta serwera.
Obudowa	Typu rack o wysokości maksymalnie 1U z możliwością instalacji do 10 dysków 2.5" Hot-Plug, z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

Procesor	Zainstalowany jeden procesor ośmiordzeniowy klasy x86 dedykowany do pracy z oferowanym serwerem, umożliwiający osiągnięcie przez oferowany serwer wyniku co najmniej 95 punktów w teście SPECrate2017_int_base według wyników publikowanych na stronie www.spec.org. Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim.
Pamięć RAM	Zainstalowane co najmniej 64 GB DDR5 RDIMM co najmniej 5600MT/s. Możliwość rozbudowy pamięci do 128 GB pamięci RAM lub więcej
Grafika	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości co najmniej 1920 x 1200
Sieć	Co najmniej: 2 interfejsy sieciowe 1Gb Ethernet w standardzie BASE-T 2 interfejsy sieciowe 10 Gb Ethernet w standardzie BASE-T
Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane co najmniej: dwa dyski Hot-Plug SAS 2,5” o pojemności co najmniej 2,4 TB każdy dwa dyski SSD SATA 2,5" o pojemności co najmniej 960 GB każdy.
Kontroler dyskowy	Sprzętowy kontroler dyskowy z nieulotną pamięcią cache co najmniej 8 GB, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
Porty	Co najmniej 3 zewnętrzne porty USB 3.x, w tym co najmniej 1 port dostępny z przodu obudowy. Co najmniej 1 port VGA.
Zasilanie	Redundantne zasilacze hotplug o mocy nie większej niż 700W każdy.
Zarządzanie	Dedykowany moduł zdalnego zarządzania, diagnostyki i monitorowania pracy serwera, niezależny od systemu operacyjnego, posiadający dedykowany port 1 GbE. Moduł musi zapewniać: • dostęp do graficznego interfejsu Web z poziomu przeglądarki internetowej, • możliwość szyfrowanego połączenia (TLS) oraz autoryzacji użytkownika, • zdalne podmontowanie napędów wirtualnych, • dostęp do wirtualnej konsoli z myszą i klawiaturą, • wsparcie dla protokołów: SNMP, IPMI 2.0, SSH, • możliwość monitorowania z jednej konsoli co najmniej 10 serwerów fizycznych,

	• wysyłanie powiadomień e-mail o awariach lub istotnych zmianach konfiguracji, • możliwość eksportu/importu konfiguracji sprzętu (BIOS, RAID, interfejsy), • możliwość przywrócenia poprzednich wersji firmware, • monitorowanie podstawowych parametrów serwera (temperatura, zasilanie, wentylatory). Możliwość zainstalowania oprogramowania producenta do zarządzania sprzętem serwerowym, które musi: • umożliwiać zarządzanie serwerami i pamięcią masową bez konieczności instalacji dedykowanego agenta, zapewniać integrację z usługą katalogową Active Directory, • obsługiwać protokoły SNMP, IPMI 2.0, SSH, Redfish, • umożliwiać harmonogramowane wykrywanie urządzeń oraz ich podstawową inwentaryzację, • zapewniać generowanie raportów (CSV, PDF) oraz alertów o zmianach stanu, • umożliwiać grupowanie urządzeń i definiowanie ról administratorów, • umożliwiać zdalną aktualizację oprogramowania sprzętowego serwerów, • być dostarczane jako obraz maszyny wirtualnej (appliance) kompatybilny z Hyper-V, umożliwiać zarządzanie dziesięcioma lub więcej urządzeń fizycznych z jednej konsoli.
Bezpieczeństwo, diagnostyka	• Blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Front obudowy serwera musi umożliwiać jednoznaczną ocenę stanu pracy urządzenia poprzez zestaw diodowych wskaźników LED, prezentujących co najmniej: status zasilania, stan systemu, aktywność sieci, błędy krytyczne, stan dysków.
System operacyjny	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 10 i wyższych. c. Zdalna dystrybucja oprogramowania na stacje robocze. d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

	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) 24. 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. 25. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 26. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 27. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 28. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 29. Zorganizowany system szkoleń i dostępne materiały edukacyjne w języku polskim. Zaoferowana wraz z serwerem licencja na system operacyjny: 30. Musi zostać tak dobrana, aby była zgodna z zasadami licencjonowania producenta i pozwalała na legalne używanie na oferowanym serwerze, 31. musi obejmować najnowszą wersję systemu dostępną na dzień składania oferty oraz uprawniać do instalacji wersji poprzedniej (tzw. *downgrade*), 32. musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego, 33. musi obejmować licencje dostępowe dla 25 użytkowników, jeśli takie licencje są wymagane przez producenta do dostępu do oprogramowania serwerowego. Wymagane dostarczenie nośników instalacyjnych umożliwiających instalację zarówno najnowszej, jak i poprzedniej wersji systemu. Do oferty należy załączyć potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym (wydruk ze strony

	producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim).
Wymagania środowiskowe	Oferowany serwer musi być zgodny z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych. Do oferty należy załączyć deklarację zgodności z dyrektywą RoHS.
Warunki gwarancyjne, wsparcie techniczne	Co najmniej pięcioletnia gwarancja producenta, obejmująca wszystkie komponenty serwera wchodzące w skład oferowanej konfiguracji. Usługi serwisu gwarancyjnego muszą być realizowane w miejscu instalacji urządzenia. Czas reakcji serwisu - do końca następnego dnia roboczego. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. Możliwość zgłaszania awarii w języku polskim poprzez ogólnopolską linię telefoniczną producenta oraz dedykowany polskojęzyczny portal techniczny producenta. W czasie obowiązywania gwarancji na sprzęt, możliwość weryfikacji - na podstawie numeru seryjnego urządzenia - pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. Usługa realizowana przez portal producenta.

1.2 Zakup NAS z dyskami

Obszar wymagań	**Wymagania minimalne**
Budowa	Obudowa wolnostojąca typu desktop Redundantne wentylatory
Procesor	Wielordzeniowy procesor 64-bitowy, uzyskujący wynik co najmniej 7 500 punktów w teście PassMark - CPU Mark według wyników dostępnych na stronie http://www.cpubenchmark.net 30 dni przed terminem składania ofert lub później. Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim.
Pamięć RAM	Zainstalowane co najmniej 16 GB pamięci RAM z możliwością rozbudowy do 32 GB lub więcej
Obsługa dysków	Ilość kieszeni dysków: co najmniej 8 (możliwość rozbudowy do 18 dysków z wykorzystaniem jednostki rozszerzającej lub równoważnie obudowa na 18 dysków). Obsługiwane typy dysków: 3,5” SATA HDD, 2,5” SATA SSD.

Zamontowane dyski	Zainstalowane co najmniej 4 dyski o pojemności co najmniej 8 TB każdy Dyski przeznaczone do pracy ciągłej 24/7, wspierające technologie korekcji błędów, z deklarowaną przez producenta średnią bezawaryjnością (MTBF) co najmniej 2 milionów godzin oraz z gwarancją producenta co najmniej 60 miesięcy Dyski muszą posiadać pamięć podręczną co najmniej 256 MB każdy Oferowane dyski muszą znajdować się na liście kompatybilności producenta NAS
RAID	Obsługa RAID co najmniej: Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6 i RAID 10. Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Funkcje i usługi	Wsparcie dla wirtualizacji Scentralizowana pamięć masowa na dane Kopia zapasowa Udostępnianie i przywracanie systemu po awarii Mechanizm szyfrowania sprzętowego Uprawnienia listy kontroli dostępu systemu Windows (ACL) Wymagana kompatybilność z usługą katalogową serwera Windows (możliwość logowania użytkowników domeny za pośrednictwem protokołów SMB/FTP/WebDAV/File Station).
Porty	Co najmniej 2 porty 1GbE RJ-45 Co najmniej 1 port 10GbE RJ-45 Co najmniej 3 porty USB 3.x Co najmniej 1 port rozszerzenia
Zasilanie	Zasilacz wewnętrzny o mocy maksymalnej nie przekraczającej 300 W Obsługa współpracy z sieciowymi zasilaczami awaryjnymi UPS
Bezpieczeństwo	Obsługa WORM (Write Once Read Many - jeden zapis, wiele odczytów) dla folderów współdzielonych i migawek, zapora sieciowa, szyfrowanie folderu współdzielonego, szyfrowanie całego woluminu, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania), dwuetapowa weryfikacja logowania (2FA), adaptacyjna metoda logowania dla konta administratora (AMFA), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail.
Oprogramowanie	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał

	obsługę migawek, generowania sum kontrolnych, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Wymaga się zapewnienia aplikacji do realizacji chmury prywatnej, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI, a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Ww. usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ww. usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników. Usługa musi być dostępna bez dodatkowych opłat, co najmniej w okresie gwarancji na urządzenie. • Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego. • Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync • Obsługa minimum 1024 migawek na folder współdzielony i minimum 65000 migawek na cały system • Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 40 jednoczesnych połączeń
Gwarancja	Gwarancja producenta co najmniej 60 miesięcy. Dopuszcza się objęcie dysków osobną gwarancją producenta dysków.

1.2 Zakup licencji oprogramowania backup

Obszar wymagań	**Wymagania minimalne**
Licencja	Wymagane dostarczenie licencji wieczystej zapewniającej ochronę 1 maszyny wirtualnej i 4 maszyn fizycznych oraz do korzystania ze wsparcia producenta przez okres od dnia odbioru do 30.06.2026
Wymagania ogólne	Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oprogramowanie musi współpracować z infrastrukturą VMware

	oraz Microsoft Hyper-V. Wszystkie niżej wskazane funkcjonalności muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba że wyszczególniono inaczej Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS 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 takiej puli. 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 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.
Wymagania RPO	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. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son). Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi – wymagane co najmniej wsparcie dla serwera kopii zapasowych – deduplikatora danych będącego przedmiotem zamówienia.

	Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 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)
Wymagania RTO	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 i Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dodatkowo dla środowiska vSphere i Hyper-V 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 i Oracle 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 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 i Linux. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. 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 SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku pointin-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.
Wymagania ograniczenia ryzyka	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 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 ESET Endpoint Antivirus. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
Wymagania dla agenta	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. Rozwiązanie musi wspierać system operacyjny macOS. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux. 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 Active Directory, Microsoft SQL. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere i Hyper-V. 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 – 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 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.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

	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.
Raportowanie	System musi umożliwiać raportowanie środowiska wirtualizacyjnego Vmware – 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 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

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

	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

Część II. Dostawa oprogramowania klasy DLP

Obszar wymagań	Wymagania minimalne
Licencja	Licencja wieczysta On-prem, min. 25 użytkowników, serwis producenta do 30.06.2026
Architektura	Architektura serwer-klient, gdzie komunikacja serwera administracyjnego z klientem odbywa się przy pomocy agenta instalowanego na stacji końcowej
Wymagania ogólne	1. System operacyjny: a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi c. MacOS 12 lub nowszy. 2. Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych. 3. Serwer administracyjny musi obsługiwać bazy danych: a. MS SQL Server 2016 lub nowsze, b. MS SQL Express, c. AzureSQL S3 lub nowsze. 4. Pomoc i dokumentacja programu dostępne co najmniej w języku angielskim. 5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim. 6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta. 7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych. 8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym. 9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia. 10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli. 11. System musi posiadać mechanizm usuwający najstarsze informacje, gdy rozmiar bazy osiągnie domyślny limit. 12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania. 13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

	14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu). 15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory. 16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym. 17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa. 18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach. 19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików. 20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych. 21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email. 22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu. 23. Serwer administracyjny musi posiadać możliwość połączenia z serwerem SMTP udostępnianym przez producenta. 24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików. 25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku. 26. Administrator musi mieć możliwość tworzenia kategorii danych dla plików zaszyfrowanych lub dla takich gdzie zawartość pliku jest niemożliwa do odczytania. 27. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp. 28. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych,

	numer PESEL, numer dowodu osobistego, numer paszportu, numer REGON, NIP, wyrażenia regularne, określone ciągi znaków i numer IBAN. 29. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym. 30. Administrator musi mieć możliwość wyszukiwania danych wrażliwych w zasobach lokalnych 31. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM. 32. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP. 33. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania. 34. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365. 35. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams. 36. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach. 37. System musi umożliwiać synchronizacji grup bezpieczeństwa z Active Directory na potrzeby logowania do konsoli zarządzającej. 38. System musi umożliwiać administratorowi nadanie użytkownikowi uprzywilejowanego dostępu, przez co nie będzie obejmowany politykami przez określony czas – 1 godzinę, 6 godzin lub do końca dnia. 39. System musi posiadać możliwość tworzenia polityk dynamicznych, pozwalających na dostosowywanie się akcji (takich jak zapisywanie logu, powiadomienie użytkownika, blokowanie lub blokowanie z możliwością zastąpienia przez użytkownika) w zależności od profilu pracy użytkownika wykonującego daną czynność, gdzie akcja dobierana jest w zależności od wyniku systemu uczenia maszynowego. 40. System musi umożliwiać dostosowanie polityk dynamicznych do dwóch trybów: standardowy oraz łagodny. Możliwość taka musi istnieć per użytkownik. 41. System musi umożliwiać tworzenie raportów na podstawie logów zebranych w układach danych z możliwością dostosowania filtrów, użytkowników oraz zakresu czasu objętych raportowaniem. 42. System musi umożliwiać utworzenie raportu, który będzie zawierał podsumowanie stanu zabezpieczenia danych wraz z rekomendacjami w formie cyklicznej.

	43. System musi zbierać informacje na temat podłączanych urządzeń do komputera, odwiedzanych domen internetowych, ścieżek sieciowych, drukarek lokalnych oraz sieciowych, umożliwiając jednocześnie przypisanie takowych wpisów do bezpiecznych lub niezaufanych lokalizacji bez potrzeby manualnego wpisywania ścieżek lub numerów seryjnych urządzeń. 44. Dla każdej z wyżej wymienionych lokalizacji system powinien umożliwiać przypisanie indywidualnej polityki dostępu – np. umożliwiając przesyłanie danych do lokalizacji oznaczonej jako bezpieczna, jednocześnie blokując wysyłkę do lokalizacji oznaczonej jako niezaufana lub nieprzypisana. 45. System musi umożliwiać audyt operacji wykonywanych przez administratora w obszarze konsoli DLP. 46. System musi umożliwiać podłączenie archiwa logów w formacie plików o rozszerzeniu mdf

Część III. Dostawa oprogramowania do zarządzania infrastrukturą IT

Obszar wymagań	**Wymagania minimalne**
Licencja	Bezterminowa, min. 25 stacji roboczych
Serwis	Aktualizacje i pomoc techniczna do 30.06.2026 r.
Wymagania ogólne	1. Oprogramowanie musi składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. 2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana powinna być przy użyciu szyfrowanego protokołu TLS 1.2. 3. Oprogramowanie musi umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych. 4. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów - nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników. 5. Oprogramowanie musi posiadać funkcjonalność monitorowania infrastruktury serwerowej i sieciowej w zakresie: a. wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping), b. wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci, c. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie. d. serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów, e. serwerów pocztowych: - monitorowanie serwisu odbierającego, jak i wysyłającego pocztę, - możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), - możliwość wykonywania operacji testowych, - możliwość wysłania powiadomienia, jeśli serwer pocztowy nie działa, f. monitorowania serwerów WWW i adresów URL, g. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail. h. obsługi komunikatów syslog i pułapek SNMP. i. monitoringu routerów i przełączników wg: - zmian stanu interfejsów sieciowych, - ruchu sieciowego, - podłączonych stacji roboczych - ruchu generowanego przez podłączone stacje robocze,

	j. kontroli nad monitorem usług Windows, k. monitorowania wydajności systemów Windows: - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. 6. Oprogramowanie musi umożliwiać automatyczne gromadzenie danych o sprzęcie i oprogramowaniu na stacjach roboczych w zakresie: a. informacji dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.; zestawienia posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade; c. informacji o zainstalowanych aplikacjach oraz aktualizacjach Windows, umożliwiających audytowanie i weryfikację użytkowania licencji w organizacji; d. informacji o wszystkich zmianach przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.; e. możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera; f. możliwość odczytania numeru seryjnego (klucze licencyjne); g. możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych; h. możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. 7. Oprogramowanie musi mieć możliwość prowadzenia bazy ewidencji majątku IT w zakresie: a. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji; b. definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości – dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz, możliwość importu danych z zewnętrznego źródła np. (.CSV);

	c. generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania; d. archiwizacji i porównywania audytów środków trwałych; e. tworzenia kodów kreskowych w Środkach Trwałych; f. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy; g. inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej co najmniej na system Android; h. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji dodatkowego oprogramowania poprzez manualne wykonanie skanów inwentaryzacji offline). 8. Oprogramowanie musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez: a. skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie, archiwów ZIP; b. zarządzanie posiadanymi licencjami; c. audyt legalności oprogramowania oraz powiadamianie w razie przekroczenia liczby posiadanych licencji; d. zarządzanie posiadanymi licencjami: raport zgodności licencji; e. możliwość przypisania do programów numerów seryjnych, wartości itp. 9. W zakresie kontroli dostępu do danych system musi umożliwiać: a. automatyczne nadawanie użytkownikowi domyślnej polityki monitorowania i bezpieczeństwa; b. ograniczenie ryzyka wycieku strategicznych danych za pośrednictwem przenośnych pamięci masowych oraz urządzeń mobilnych; c. zabezpieczenie sieci firmowej przed wirusami instalującymi się automatycznie z pendrive'ów lub dysków zewnętrznych; d. integracja z Windows Defender: zarządzanie ustawieniami wbudowanego antywirusa wraz z możliwością alarmowania o wykrytych problemach oraz wynikach skanowania; e. integracja z Windows Firewall: włączanie i wyłączanie zapory dla wybranych typów połączeń, tworzenie reguł ruchu, odczyt stanu zapory na stacjach roboczych; f. możliwość usuwania nieistniejących/zutylizowanych nośników danych (np. USB); g. alarmy o podłączonym urządzeniu obcym (nieposiadającym atrybutu „nośnik zaufany”);

	h. integracja z Windows Bitlocker: odczyt stanu modułu TPM oraz zaszyfrowania woluminów i. zdefiniowanie polityki przenoszenia danych firmowych przez pracowników wraz z odpowiednimi uprawnieniami; j. informacje o urządzeniach podłączonych do danego komputera; k. lista wszystkich urządzeń podłączonych do komputerów w sieci; l. audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz na udziałach sieciowych; m. zarządzanie prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników; n. centralna konfiguracja: ustawienie reguł dla całej sieci, dla wybranych map sieci oraz dla grup i użytkowników Active Directory.

Część IV. Zakup modułu XDR do ESET Protect

Obszar wymagań	**Wymagania minimalne**
Opis	Przedmiotem zamówienia jest podniesienie wersji oprogramowania antywirusowego do wersji z XDR. Obecnie Zamawiający posiada **30 szt**. licencji na oprogramowanie ESET PROTECT Advanced. Rodzaj licencji: Podniesienie istniejących licencji na oprogramowanie antywirusowe ESET PROTECT Advanced ON-PREM do wersji ESET PROTECT Elite Obecna ilość licencji: 30 szt. Okres licencjonowania: do dnia 15.11.2026. Obecnie posiadana licencja jest ważna do 15.11.2026

Wójt Gminy
Sławomir Kruśliński

Sławomir Mieczysław Kruśliński

Elektronicznie podpisany przez Sławomir Mieczysław Kruśliński
Data: 2025.12.04 11:55:28 +01'00'