Oprogramowanie wraz z wdrożeniem

1. **VMware vSphere 7 Essentials Plus Kit** dla 3 hostów – (maksymalnie po 2 procesory na hosta) **z wdrożeniem i migracją.**

licencja wraz z podstawowym rocznym wsparciem na ww. produkt.

Poprzez „wdrożenie i migrację" Zamawiający rozumie uruchomienie dostarczonego oprogramowania i migrację do niego systemu istniejącej struktury będącej w wersji 5.5.

Ogólny opis wdrożenia i migracji	
Lp.	**Zakres prac do wykonania**
1.	Aktualizacja firmware komponentów sprzętowych klastra (Dell PE M1000e): • aktualizacja firmware macierzy oraz oprogramowania do zarządzania macierzami, • aktualizacja firmware serwerów do zalecanych przez producenta wersji, • aktualizacja switchy MXL zainstalowanych w obudowie, • aktualizacja modułów zarządzających obudową.
2.	Rekonfiguracja switchy na potrzeby klastra iSCSI jeśli jest wymagana po zmianie wersji firmware.
3.	Aktualizacja wersji Wmware vSphere z 5.5: • aktualizacja vCenter server do najnowszej produkcyjnej wersji zalecanej dla posiadanego sprzętu, • aktualizacja hostów esxi klastra do zalecanej wersji, • konfiguracja update managera i aktualizacja elementów klastra do najnowszych dostępnych wersji poprawek, • podniesienie wirtualnego hardware maszyn wirtualnych oraz narzędzi VMTools.
4.	Weryfikacja działania klastra (vmotion, HA).
5.	Wykonanie dokumentacji rozwiązania.
6.	Przeprowadzenie szkolenia w siedzibie Zamawiającego dla 4 administratorów – pracowników Wydziału Informatyki i Cyberbezpieczeństwa w oparciu o wdrożony, uruchomiony i przetestowany system.
Uwaga! Ww. prace należy prowadzić w stopniu jak najmniej zakłócającym pracę Systemu Informatycznego Starostwa, a potencjalne wyłączenia lub braki dostępności usług należy zaplanować w taki sposób, aby miały miejsce poza godzinami pracy Starostwa Powiatowego w Cieszynie. Szczegóły dotyczące zakresu usługi będą na bieżąco uzgadniane z pracownikami Wydziału Informatyki i Cyberbezpieczeństwa na etapie realizacji.	

2. **Oprogramowanie do zabezpieczenia danych (wykonywania kopii zapasowych) wraz z wdrożeniem i migracją.**

licencja wraz z minimum podstawowym 5-letnim wsparciem na zaoferowany produkt

Lp.	**Cechy/minimalne wymagania**

1.	Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia systemu do zabezpieczania środowiska Data Center (baz danych, maszyn wirtualnych, serwerów wolnostojących) wraz z migracją istniejących zadań wykonywanych w systemie Veritas Backup Exec 16.
2.	Wymagane jest dostarczenie modułów oprogramowania: • backupowego (aplikacja backupowa), • umożliwiającego stworzenie systemu raportującego, • umożliwiającego zaindeksowanie oraz przeszukiwanie danych backupowych, • umożliwiającego stworzenie rozwiązania Continuous Data Protection (CDP) dla środowisk VMware, • umożliwiającego konfigurację/instalację deduplikatora, • umożliwiające zarządzanie oferowanym środowiskiem dedykowanym do zabezpieczania danych. Oferowane oprogramowanie powinno spełniać wszystkie wymienione w niniejszej tabeli funkcjonalności. Wymagane wsparcie na oferowane oprogramowanie realizowane przez producenta w okresie min. 5 lat w trybie 9x5 NBD, gwarantujące dostęp do najnowszych wersji oprogramowania.
3.	Wymagane jest dostarczenie licencji w/w oprogramowania do zabezpieczania danych dla środowiska obejmującego zarówno serwery niezwirtualizowane oraz zwirtualizowane, charakteryzujące się sumaryczną ilością: 10 CPU. Zamawiający przewiduje w kolejnych latach rozbudowę zabezpieczanego środowiska, dlatego wymagana jest możliwość skalowania rozwiązania stworzonego w oparciu o licencje będące przedmiotem zapytania - poprzez dokładanie kolejnych licencji, co powinno umożliwić zabezpieczenie środowiska o sumarycznej ilości 50 CPU, bez względu na rozmiar zabezpieczanego wolumenu danych. Licencje będące przedmiotem zapytania powinny umożliwić skonfigurowanie deduplikatora o pojemności nie mniejszej niż 20 TB netto oraz umożliwić zabezpieczenie co najmniej 75 maszyn wirtualnych (min. vSphere 6.5) w trybie CDP.

Wymagania dotyczące aplikacji backupowej:

Lp.	**Cechy/minimalne wymagania**
1.	Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE, Debian, CentOS, Ubuntu), Solaris, AIX, HP-UX, FreeBSD. Backup zasobów plików w przypadku powyższych systemów musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z przedstawionymi wymaganiami.
2.	Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych i aplikacji: MS Exchange, MS SQL, Oracle, IBM DB2, Lotus Notes, SharePoint, SAP, Sybase, VMware, HyperV. Backup powyższych baz danych i aplikacji musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z przedstawionymi wymaganiami.
3.	W przypadku zabezpieczania baz danych i aplikacji wymagana możliwość realizacji kopii zapasowej kilkoma strumieniami jednocześnie (minimum 10 jednoczesnych strumieni).

4.	Oferowane rozwiązanie musi zabezpieczać zde-duplikowane dane w przypadku systemu Windows 2012 bez konieczności przywracania danych Windows 2012 do postaci oryginalnej (nie zde-duplikowanej).
5.	Zabezpieczane serwery muszą być backupowane bezpośrednio na dyski de-duplikatora (zainstalowanego/skonfigurowanego w oparciu o licencje będące przedmiotem zapytania) bez pośrednictwa jakichkolwiek innych urządzeń/serwerów, dostarczone licencje (dotyczy aplikacji backup'owej oraz deduplikatora) powinny umożliwiać całkowitą utylizację wymaganej przestrzeni deduplikatora.
6.	Transfer danych z zabezpieczanych serwerów do oferowanego de-duplikatora nie może się odbywać po sieci SAN.
7.	Oprogramowanie backupowe musi umożliwiać dla sieci lokalnej: • backup pojedynczych plików, • backup całych systemów plików, • backup baz danych w trakcie ich normalnej pracy, • backup ustawień systemu operacyjnego Windows, • backup całych obrazów maszyn wirtualnych systemu VMware, • backup całych obrazów maszyn wirtualnych systemu HyperV.
8.	Rozwiązanie backupowe musi umożliwiać transfer danych bezpośrednio ze zdalnych lokalizacji do oferowanego deduplikatora bez konieczności instalacji jakiegokolwiek sprzętu w lokalizacji. Powyższa funkcjonalność wymagana jest dla następujących typów danych: • backup pojedynczych plików, • backup całych systemów plików, • backup baz danych w trakcie ich normalnej pracy.
9.	W przypadku zabezpieczania środowisk zdalnych, oferowane rozwiązanie backupowe nie może wymagać zaangażowania ze strony personelu.
10.	Wymaga się aby oferowane rozwiązanie backupowe było w pełni konfigurowalne ze zdalnej konsoli, w szczególności backupy maszyn (bazy, pliki) czy też backupy laptopów muszą być konfigurowalne z poziomu centralnej konsoli bez konieczności logowania się na zabezpieczaną maszynę.
11.	Oferowane rozwiązanie backupowe musi umożliwiać odtworzenie • plików, • baz danych, na docelową maszynę w lokalizacji z poziomu centralnej konsoli systemu backupowego. Wymagany scenariusz nie może wymagać logowania się na odtwarzaną maszynę w celu odtworzenia danych z systemu backupowego.
12.	W celu minimalizacji ilości przesyłanych danych, oferowane rozwiązanie musi mieć możliwość przesyłania odtwarzanych danych do docelowego serwera w postaci skompresowanej, odtwarzane dane powinny zostać rozkompresowane na docelowym serwerze przez agenta oferowanego systemu.
13.	Oprogramowanie backupowe musi posiadać funkcjonalność podziału danych (plików, baz danych, obrazów maszyn wirtualnych) na bloki o zmiennej długości. System musi się dopasowywać do struktury dokumentu zapewniając podział na bloki o różnej długości w ramach pojedynczego dokumentu w celu polepszenia efektywności de-duplikacji.

	Podział na bloki musi następować bezpośrednio na zabezpieczanym serwerze.
14.	Używany algorytm de-duplikacji musi również generować zmienny blok w przypadku backupu pojedynczego dokumentu. Bloki wysyłane w trakcie backupu pojedynczego dokumentu (z zabezpieczanej maszyny do medium de-duplikacyjnego) muszą być różnej długości jednak nie większej niż 32kB.
15.	Każdy backupowany dokument w trakcie pojedynczej sesji musi być dzielony na bloki o zmiennej długości nie większej niż 32kB.
16.	Wymaga się aby oprogramowanie backupowe przesyłało na oferowany deduplikator tylko unikalne bloki nie znajdujące się na tym urządzeniu, w efekcie skracając czas backupu, obciążenie procesora i zmniejszając ruch w sieci WAN / LAN.
17.	Funkcjonalność deduplikacji nie może wymagać instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera backupowego.
18.	Oprogramowanie backupowe nie może odczytywać tych plików z systemu dyskowego, które się nie zmieniły w stosunku do ostatniego backupu. Raz zbackupowany plik nie może być ponownie odczytywany, chyba, że zmieni się jego zawartość.
19.	Wymaga się aby oprogramowanie backupowe realizowało wyłącznie - logicznie pełne backupy systemu plików. Z zabezpieczanego systemu plików muszą odczytywane tylko nowe lub zmienione pliki, do oferowanego de-duplikatora powinny być przesyłane dane po de-duplikacji, jednak każdy finalny backup musi być logicznie pełnym backupem. W wewnętrznej strukturze systemu musi być przechowywana informacja o każdym backupie i należących do niego danych (blokach), dzięki czemu odtworzenie jakichkolwiek danych plikowych musi być pojedynczym zadaniem identycznym z odtworzeniem danych z pełnego backupu.
20.	Wymagana możliwość definiowania w konsoli oprogramowania backupowego ważności (retencji) danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte.
21.	Wymagana możliwość tworzenia z poziomu GUI (konsoli graficznej) w przypadku oferowanego oprogramowania backupowego, polityk typu „dziadek – ojciec –syn”, to znaczy tworzenia polityk w których zdefiniowano: • czas przechowywania backupów dziennych, • czas przechowywania backupów tygodniowych, • czas przechowywania backupów miesięcznych, • czas przechowywania backupów rocznych.
22.	Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego. Wymagana możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów: • wybranych typów plików, np. dla plików z rozszerzeniem mp3, • dla całych katalogów (np.: c:\windows), • dla pojedynczych plików.
23.	Oferowane rozwiązanie musi mieć możliwość zdefiniowania aby ostatni backup dowolnego zbioru danych nigdy się nie przeterminował. Oznacza to, że jeśli dany zasób nie jest backupowany to automatycznie ostatni ważny backup tego zasobu będzie przechowywany bezterminowo, jedynie administrator może zdecydować o jego usunięciu.

24.	Konsola zarządzająca systemem backupowym musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról (min, administrator, monitoring, tylko wykonywanie odtworzeń) w systemie backupowym.
25.	Wymagana możliwość generowania (poprzez konsolę) raportów określających zajętość przestrzeni przeznaczonej na składowanie de-duplikatów.
26.	Bloki przesyłane z zabezpieczanych serwerów do oferowanego de-duplikatora muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256-bitowym.
27.	Wymagana możliwość szyfrowania danych na medium dyskowym przechowującym backupy (de-duplikaty). Ewentualna licencja szyfrowania nie musi być dostarczona w ramach postępowania.
28.	Wymagana jest autentykacja komunikacji między klientem a serwerem backupu (farmą serwerów) oparta na certyfikatach.
29.	Oprogramowanie backupowe musi pozwalać na odtwarzanie danych poprzez: wybór odtwarzanych danych, odtworzenie danych w jednym kroku.
30.	Wymagana możliwość limitowania wielkości zadania backupowego, jeśli zadanie backupowe przekroczy zdefiniowaną wielkość wówczas nie może być zapisane w systemie backupowym.
31.	Oprogramowanie backupowe musi umożliwiać ograniczenie mocy procesora używanej do wykonywania zdania backupu tak aby odpowiednia moc procesora pozostała do wykorzystania dla innych zadań.
32.	Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware 6.0, 6.5,6.7, 7.0. Oprogramowanie backupowe musi umożliwiać w przypadku środowisk VMware następujące typy backupu: a. backup całych maszyn wirtualnych, b. backup pojedynczych, wybranych dysków maszyny wirtualnej vmdk, c. musi istnieć możliwość zastosowania wyrażeń regularnych do określenia które wirtualne dyski VMware mają być backupowane, d. w trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn systemu VMware (wymagane wykorzystanie mechanizmu CBT systemu VMware), e. wykonywanie backupu obrazów maszyn wirtualnych VMware nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk). Powyższe metody backupu maszyn wirtualnych muszą podlegać deduplikacji ze zmiennym blokiem przed wysłaniem danych do medium backupowego zgodnie z przytoczonymi wymaganiami dla de-duplikacji. Powyższe metody backupu muszą być wbudowane w oferowany system backupu, nie powinny wymagać tworzenia skryptów/dodatkowych komend.
33.	Oferowany system musi pozwalać na szybkie odtworzenie • całych obrazów maszyn wirtualnych, • pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej.
34.	Wymaga się aby oferowane rozwiązanie backupowe umożliwiało odtwarzanie obrazów maszyn wirtualnych VMware z następującymi funkcjonalnościami:

	a. odtwarzanie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu, b. odtwarzanie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu, c. odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej, funkcjonalność ta musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux, d. możliwość zamontowania na dowolnym serwerze (fizycznym lub wirtualnym) zbackupowanych obrazów maszyn wirtualnych Windows (plików vmdk maszyny wirtualnej Windows), w efekcie metoda ta nie odtwarza backupów a jedynie umożliwia na przeglądanie zawartości plików vmdk w backupie z poziomu Eksploratora Plików Windows na dowolnej maszynie. Powyższe metody odtworzenia muszą być wbudowane w system backupu i w pełni automatyczne nie mogą generować konieczności wykorzystania dodatkowych skryptów/ komend.
35.	Oferowane oprogramowanie backupowe musi mieć możliwość prezentacji (bez konieczności odtworzenia) zbackupowanych obrazów maszyn wirtualnych VMware (plików vmdk) jako katalogów na maszynie fizycznej w celu ich przeszukiwania (wymagane przeszukiwanie po nazwach plików jak również zawartości plików) z poziomu systemu operacyjnego maszyny fizycznej.
36.	Oferowane oprogramowanie backupowe musi mieć możliwość backupu/odtworzenia w trybie „image backup” (backup plików vmdk) maszyn wirtualnych znajdujących się na serwerach VMware ESX bez udziału vCenter.
37.	Oferowane oprogramowanie backupowe musi mieć możliwość automatycznego sprawdzania (weryfikacji) zbackupowanych maszyn wirtualnych VMware, wymagana możliwość ustawienia kalendarza weryfikacji maszyn wirtualnych VMware. Weryfikacja maszyn wirtualnych musi zapewniać minimum: a. odtworzenie maszyny wirtualnej na zdefiniowanym Data Center/Data Store, b. weryfikację podstawowych procesów, c. możliwość dołączenia własnego skryptu weryfikującego wybrane elementy maszyny wirtualnej. Wymagana dostępność informacji w konsoli systemu backupu o statusie (poprawna/niepoprawna) weryfikacji maszyny wirtualnej.
38.	Administrator (właściciel) danej maszyny wirtualnej VMware musi mieć możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy tez administratorem VMware) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej.
39.	Oprogramowanie backupowe musi zawsze przechowywać pełne backupy obrazów maszyn wirtualnych środowiska VMware dla każdej wykonanej w przeszłości kopii zapasowej. Każdy backup obrazu maszyny wirtualnej musi być backupem pełnym.
40.	Oferowane rozwiązanie backupowe musi umożliwiać na tworzenie automatycznych polityk backupowych dla: • folderu,

	• resource pool systemu VMware. Oznacza to, że dodanie maszyny wirtualnej do folderu, hosta czy resource pooli w systemie VMware spowoduje automatyczne backupowanie dodanej maszyny wirtualnej zgodnie z polityka zdefiniowana dla folderu hosta czy resource pooli w systemie VMware.
41.	Rozwiązanie backupowe musi umożliwiać zdefiniowanie polityk backupowych dostępnych dla administratora systemu VMware z poziomu vCenter. Administrator VMware musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do polityk backupowych.
42.	Oferowany system musi automatycznie naprawiać problemy związane ze snapshotami VMware. W przypadku gdy system VMware nie usunie snapshotu, oprogramowanie backupowe musi automatycznie ponawiać usunięcie snapshotu a w przypadku konieczności automatycznie konsolidować maszyny wirtualne VMware.
43.	Wymaga się aby inicjowanie backupu oraz odtwarzanie maszyn wirtualnych VMware dostępne było z poziomu graficznego interfejsu, linii komend oraz przez REST API.
44.	Oferowane oprogramowanie backupowe powinno umożliwiać dla środowisk Hyper-V: a. backup pojedynczych plików i baz danych z maszyny wirtualnej ze środka maszyny wirtualnej Hyper-V, b. backup całych maszyn wirtualnych (czyli plików vhd reprezentujących wirtualną maszynę), takie wykonanie backupu nie powinno wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vhd), c. wykonywanie backupu jak w punkcie b. powinno umożliwiać na odtworzenie pojedynczych plików z obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej, funkcjonalność ta powinna być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows, − dopuszcza się wykonywanie snapshotów vss maszyn wirtualnych i użycie ich w trakcie backupu obrazów maszyn wirtualnych, − powyższe metody backupu muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend, − powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji ze zmiennym blokiem w momencie odczytu danych zgodnie z wymaganiami powyżej.
45.	Oferowane oprogramowanie backupowe musi zapewniać spójny backup Exchange / MSSQL przy backupie obrazów maszyn wirtualnych środowiska Hyper-V.
46.	Wymagana możliwość odtworzenia danych: • z zabezpieczanego serwera / komputera, • z konsoli systemu backupowego.
47.	Wymagana możliwość odtworzenia: • pojedynczego pliku, • zabezpieczanej bazy danych.

48.	W przypadku systemów Windows 2012, 2016 wymagana funkcjonalność Bare Metal Recovery - automatycznego odtworzenia całego serwera (system operacyjny + ustawienia systemu operacyjnego + dane) w jednym kroku bezpośrednio z oferowanego urządzenia. Funkcjonalność ta powinna być wbudowana w rozwiązanie backupowe.
49.	W przypadku odtwarzania danych poprzez interfejs dostępny na zabezpieczanym serwerze/laptopie wymagany mechanizm autentykacji użytkowników spełniający funkcjonalności: • mechanizm wbudowany w system backupowy, • mechanizm zintegrowany z usługami katalogowymi, • w przypadku wykorzystania AD, użytkownicy będący w domenie nie muszą się logować do systemu backupu w przypadku konieczności: i. odtworzenia danych, ii. przeszukania zwartości swoich backupów, iii. wykonania backupu.
50.	W przypadku odtwarzania danych poprzez interfejs końcowego użytkownika dostępnego na zabezpieczanym laptopie/PC wymagane są następujące funkcjonalności: • możliwość wyszukiwania pliku do odtwarzania po: i. nazwie pliku, ii. początkowym fragmencie nazwy pliku, iii. końcowym fragmencie nazwy pliku, iv. fragmencie nazwy pliku umiejscowionym gdziekolwiek w pełnej nazwie pliku, • możliwość przeglądania zawartości zbackupowanego systemu plików i wybór zasobów do odtworzenia, • możliwość wyboru wersji odtwarzanego pliku / katalogu.
51.	Oferowane rozwiązanie backupowe powinno umożliwiać odtwarzanie plików z dowolnego urządzenia (laptop, tablet, smartphone) poprzez przeglądarkę internetową, odtwarzanie tego typu powinno posiadać następujące funkcjonalności: • uwierzytelnienia użytkownika, • możliwość wyszukiwania plików do odtwarzania po: i. nazwie pliku, ii. początkowym fragmencie nazwy pliku, iii. końcowym fragmencie nazwy pliku, iv. fragmencie nazwy pliku umiejscowionym gdziekolwiek w pełnej nazwie pliku, • możliwość przeglądania zawartości zbackupowanego systemu plików i wybór zasobów do odtworzenia, • możliwość wyboru wersji odtwarzanego pliku / katalogu.
52.	W przypadku odtwarzania istniejącego systemu plików (systemu plików który utracił część zasobów) oprogramowanie backupowe musi samo, automatycznie sprawdzać których plików znajdujących się w backupie, brakuje na odtwarzanej maszynie a następnie odczytać z backupu i przesłać tylko te pliki które znajdują się w backupie a których brakuje na odtwarzanej maszynie.
53.	Oferowany system backupu musi być dostępny (dla backupu i odtwarzania) przez 24h na dobę 7 dni w tygodniu, wyklucza się istnienie okresów w przypadku których system backupowy nie może wykonywać backupu lub odtwarzania (tzw. BLACKOUT WINDOWS).

54.	Wymaga się aby oferowany system backupu posiadał możliwość bezpośredniego raportowania o błędach do serwisu producenta.
55.	Oferowany system backupu powinien mieć możliwość instalacji agentów jako plików msi. Wymagana możliwość automatyzacji instalacji agentów poprzez uruchomienie skryptu na zabezpieczanej maszynie, przyporządkowującego maszynę automatycznie do określonej polityki backupowej.
56.	Oferowany system backupu powinien posiadać możliwość automatycznej samo-aktualizacji poprzez automatyczne ściąganie nowych wersji oprogramowania od producenta.
57.	Oferowany system backupu musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z serwera backupu.
W ramach oferowanych licencji wymaga się następujących funkcjonalności – dotyczących monitorowania, raportowania oraz przeszukiwania backupów:	
Lp.	**Cechy/minimalne wymagania**
1.	W ramach dostarczonych licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania z użycia komponentów systemu backupowego oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego. Wymagana dostępność następujących raportów: a. podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych), b. podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych danych), c. zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów, d. zbiorcze zestawienie zabezpieczanych serwerów które w sposób ciągły (kilka razy pod rząd) maja problem z backupami, e. zestawienie zabezpieczanych systemów plików które w ogóle nie są backupowane. f. spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii), g. najmniej wiarygodne zabezpieczanych serwery (procent nieudanych backupów), h. lista najwolniejszych/najszybszych zabezpieczanych maszyn, i. poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego, j. mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO (punktu do którego się odtwarzamy), k. liczba danych backupowanych dziennie, l. liczba zadań backupowych dziennie, m. zużycie zasobów na serwerach backupowych (procesor, pamięć, karty sieciowe LAN, SAN), n. zużycie mediów backupowych i napędów taśmowych, o. aktualna konfiguracja systemu backupowego, p. historia zmian konfiguracji systemu backupowego, q. posiadane licencje systemu backupowego,

	r. wykorzystanie systemu backupowego przez poszczególne działy / grupy użytkowników (chargeback per cost center).
2.	W ramach dostarczonych licencji wymagana możliwość zaindeksowania oraz przeszukiwania backupów z poziomu graficznego interface'u (GUI), wymagana także możliwość wyszukania dowolnych fraz w nazwach plików.
W ramach oferowanych licencji wymaga się następujących funkcjonalności – dotyczy rozwiązań Continuous Data Protection dla środowisk VMware:	
3.	Integracja na poziomie VMware vCenter Plug-in (ORCHESTRATION, MANAGEMENT) , vSphere Web Client GUI.
4.	Wsparcie dla HA, DRS, S-DRS, VMotion, S-VMotion.
5.	Możliwość integracji z VMware vRealize Operations Manager.
6.	Rozwiązanie dostarczane w postaci oprogramowania instalowanego na platformie ESXi.
7.	Zabezpieczenie dowolnej maszyny wirtualnej wraz z aplikacjami w trybie ciągłym tzn. umożliwiającym odtworzenie do dowolnego punktu w czasie (tzw. PIT – Point In Time), wymagane wsparcie dla VMware ESXi 6.0.
8.	Możliwość tworzenia tzw. CONSISTENCY GROUP zapewniających identyczną konsystencję dla przynależących do danej grupy maszyn wirtualnych (VM).
9.	Zabezpieczenie realizowane za pośrednictwem ciągłej replikacji (a nie za pomocą SNAPSHOT'ów) na poziomie VMDK oraz RDM, niezależnie od użytego storage'u (tzw. Storage Agnostic -warunkiem jest wsparcie przez VMware), wymagane wsparcie dla połączeń: FC, FCoE, iSCSI, NAS oraz DAS.
10.	Wsparcie dla replikacji (bi-directional) asynchronicznej oraz synchronicznej (realizowanej na poziomie dostarczanego oprogramowania), połączonych z mechanizmem tzw. JOURNALING umożliwiającego odnotowanie wszystkich zmian zabezpieczanego środowiska.
11.	Odporność na krótkotrwałe problemy (przeciążenie, zaniki) związane z siecią WAN.
12.	Wbudowana funkcjonalność deduplikacji oraz kompresji w przypadku transmisji danych poprzez WAN.
13.	Wsparcie dla równoległej replikacji zabezpieczanego środowiska do różnych ośrodków docelowych (min. 3-ech), wsparcie dla replikacji równoległej powinno być zapewnione również na poziomie grup konsystencji (CONSISTENCY GROUP).
14.	Proponowane rozwiązanie powinno umożliwiać: • stworzenia DISASTER RECOVERY dla całego zabezpieczanego wirtualnego środowiska zbudowanego w oparciu o VMware, • operacyjne ODTWARZANIE dowolnej maszyny VM wraz z aplikacjami , • MIGRACJI danych w trybie ON-LINE na inne zasoby dyskowe.
15.	Równoległe wsparcie środowisk lokalnych oraz zdalnych, wymagana możliwość pracy w 3-ech trybach, tzw.: CDP (Continuous Data Protection tyb replikacji lokalnej), CRR (Continuous Remote Replication tryb replikacji zdalnej), CLR (Continuous Local and Remote

	Replication połączenie CDP oraz CLR tryb replikacji lokalnej oraz zdalnej) w ramach dostarczonych licencji.
16.	Granularność umożliwiająca pominięcie określonych plików VMDK związanych z wirtualnymi serwerami VM objętych protekcją.
17.	Architektura FAULT-TOLERANT, brak pojedynczego punktu awarii.
18.	Działanie rozwiązania będącego przedmiotem zapytania nie może mieć żadnego negatywnego wpływu na wydajność zabezpieczanych maszyn i aplikacji.
19.	Wyskalowanie systemu powinno gwarantować RPO (Recovery Point Objective) w przypadku codziennej pracy ciągłej na poziomie pojedynczych sekund.
20.	Proponowana konfiguracja systemu powinna zapewnić następującą retencję przechowywanych kopii bezpieczeństwa: - RPO=30s z ostatnich 24h, - RPO=24h z ostatniego tygodnia, - RPO=1tydzień z ostatniego miesiąca.
21.	Możliwość odtworzenia zabezpieczanego środowiska do dowolnego punktu w czasie.
22.	Możliwość trybu pracy umożliwiającego objęciem protekcją w sposób automatyczny nowo dodanych maszyn wirtualnych (VM).
23.	Rozwiązanie powinno dopuszczać zmiany HW na poziomie infrastruktury zabezpieczanego środowiska bez negatywnego wpływu na działanie systemu.
24.	Możliwość użycia mechanizmu typu BOOKMARK dla oznaczenia konsystentnych kopii zabezpieczanych aplikacji.
25.	Wsparcie dla VSS, zapewnienie konsystencji aplikacji na poziomie VSS.
26.	Możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie dla określonych produkcyjnych serwerów wirtualnych (VM), w tym: odtworzenie, uruchomienie (z zachowaniem wymaganej sekwencji), konfigurację.
27.	Możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie określonych testowych maszyn wirtualnych (VM).
28.	Możliwość automatycznego zainicjowania procesu REVERSE REPLICATION w przypadku procesów FAILOVER/FAILBACK.
29.	Możliwość przeprowadzania testów DR bez wpływu na zabezpieczane serwery produkcyjne oraz bez konieczności zmian w działaniu replikacji (np.: PAUSE, REVERSE, …).
30.	Możliwość skryptowego tworzenia planów RECOVERY.
Wymagania funkcjonalne dotyczące de-duplikatora skonfigurowanego w oparciu o licencje będące przedmiotem zapytania (wymagany rozmiar de-duplikatora został podany wcześniej).	
1.	Rozwiązanie powstałe w wyniku instalacji/konfiguracji licencji będących przedmiotem zapytania musi być przeznaczone do de-duplikacji, dedykowane do przechowywania kopii zapasowych.
2.	Oprogramowanie będące przedmiotem zapytania musi umożliwiać konfigurację de-duplikatora na platformie VMware vSphere 6.5, 6.7 oraz min. Microsoft Windows Server

	2012 R2 z Hyper-V, o wcześniej określonej przestrzeni (powierzchni użytkowej dedykowanej do przechowywania deduplikatów) bez uwzględniania mechanizmów protekcji, wymagane skalowanie do min. 90TB powierzchni netto w ramach tego samego urządzenia.
3.	Deduplikator musi zapewniać jednoczesny dostęp wszystkimi poniższymi protokołami: • CIFS, • NFS, • deduplikacja na źródle (alternatywnie OST/BOOST/CATALYST), w obrębie oferowanej pojemności urządzenia.
4.	Wymagane jest dostarczenie licencji zapewniających funkcjonalność: ENCRYPTION (szyfrowanie) w obrębie maksymalnej wymaganej pojemności urządzenia.
5.	Urządzenie musi pozwalać na jednoczesną obsługę minimum 20 strumieni.
6.	Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.
7.	Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości.
8.	De-duplikacja zmiennym, dynamicznym blokiem musi oznaczać, że wielkość każdego bloku (na jakie są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego i jest indywidualnie ustalana przez algorytm urządzenia w celu maksymalnego zwiększenia efektywności de-duplikacji.
9.	Niedopuszczalna jest de-duplikacja stałym blokiem o ustalonej tej samej długości, możliwość manualnej zmiany (bądź poprzez oskryptowanie) długości bloku de-duplikacji również nie może zastąpić wymogu automatycznego doboru długości bloku na jaki dzielony jest każdy strumień danych.
10.	Oferowany produkt musi posiadać obsługę mechanizmów globalnej de-duplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, de-duplikacja na źródle) przechowywanych w obrębie całego urządzenia. W obrębie całego urządzenia, raz otrzymany i zapisany w urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany.
11.	Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej de-duplikacji pomiędzy dowolnymi dwoma udziałami NFS, CIFS. Blok danych otrzymany i zapisany na udział CIFS, nie może zostać ponownie zapisany jeśli trafi do udziału NFS w obrębie tego samego urządzenia (to samo dotyczy de-duplikacji na źródle).
12.	Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych.
13.	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo skompresowane
14.	Oferowane rozwiązanie musi wspierać oferowaną aplikację backup'ową oraz co najmniej: VERITAS NetBackup, EMC Networker, Veeam, Oracle RMAN, Microsoft SQL Server Management Studio.
15.	W przypadku współpracy z każdą z poniższych aplikacji: • RMAN (dla ORACLE), • Microsoft SQL Server Management Studio (dla Microsoft SQL), • VERITAS NetBackup, • EMC NetWorker,

	• Veeam, urządzenie musi umożliwiać de-duplikację na źródle (de-duplikację na zabezpieczanej maszynie) i przesyłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. De-duplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do oferowanego urządzenia były transmitowane poprzez sieć LAN tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu.
16.	W przypadku de-duplikacji na źródle poprzez sieć IP (LAN oraz WAN), musi być możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
17.	Urządzenie powinno dopuszczać co najmniej 90% utylizację powierzchni netto, bez widocznego spadku wydajności. Dokumentacja urządzenia nie może wskazywać na jakiekolwiek problemy czy obostrzenia, które mogą pojawić się przy zapełnieniu urządzenia poniżej 90%.
18.	Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych (bez pośrednictwa dodatkowych modułów) do drugiego urządzenia tego samego typu, wymagane następujące tryby pracy replikacji: • jeden do jednego, • wiele do jednego, • jeden do wielu, • kaskadowej (urządzenie A replikuje dane do urządzenia B które te same dane replikuje do urządzenia C). Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu, rozwiązanie replikacyjne nie powinno wymagać aby obszar na który dane są replikowane był większy od obszaru źródłowego (replikowanego) w przypadku schematu „jeden do jednego" – weryfikacja na podstawie ogólnie dostępnej dokumentacji producenta oraz zaleceń. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania.
19.	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
20.	W przypadku replikacji danych między dwoma urządzeniami kontrolowanej przez systemy: oferowaną aplikację backupową/ VERITAS NetBackup /EMC NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności: • replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących, • replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu, • replikacja zarządzana jest z poziomu aplikacji backupowej, aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji.
21.	Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%.
22.	Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.
23.	Deduplikator musi umożliwiać wykonywanie oraz przechowywanie SnapShot'ów (min. 50 jednocześnie), czyli możliwość zamrożenia obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane rozwiązanie musi również umożliwiać odtworzenie danych ze Snapshot'u. Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania backupów / odtwarzania).

24.	Deduplikator musi pozwalać na podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą de-duplikowane (globalna de-duplikacja między logicznymi częściami urządzenia).
25.	Deduplikator musi mieć możliwość podziału na minimum 14 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 14 logicznych części pracujących równolegle z pełną wydajnością urządzenia.
26.	Dla każdej z logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią de-duplikatora. Użytkownicy zarządzający logiczną częścią muszą widzieć tylko i wyłącznie zasoby logicznej części i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia.
27.	Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego rozwiązania, jako niezależnego urządzenia dostępnego poprzez: • CIFS, • NFS, • wymagany protokół umożliwiający de-duplikację na źródle.
28.	Rozwiązanie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.
29.	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu), nie może wymagać (zgodnie z oficjalnymi zaleceniami producenta) definiowania BLACKOUT WINDOW czyli okna czasowego dedykowanego dla procesu czyszczenia podczas którego nie są realizowane procesy backupu / odtwarzania danych czy replikacji.
30.	Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).
31.	Wymagana możliwość zdefiniowania czasu, w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia).
32.	Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas, w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta).
33.	Rozwiązanie musi mieć możliwość zarządzania poprzez • interfejs graficzny dostępny z przeglądarki internetowej, • poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell).
Wymagania funkcjonalne dotyczące środowiska umożliwiającego zarządzanie środowiskiem dedykowanym do zabezpieczania danych stworzonego w oparciu o oprogramowanie będące przedmiotem zapytania	
1.	Możliwość uruchomienia zdalnych konsol dla: • aplikacji backup'owej, • systemu dedykowanego do raportowania, • systemu dedykowanego do przeszukiwania danych backup'owych, • systemu CDP, • de-duplikatorów, stworzonych w oparciu o oprogramowanie będące przedmiotem zapytania, możliwość zdalnego uruchomienia oraz wyłączenia w/w komponentów
2.	Zapewnienie podglądu on-line takich elementów jak: • aktywność procesów backup'owych, • aktywność procesów replikacyjnych,

	• aktualny status, • alarmy, w przypadku zaoferowanej aplikacji backup'owej oraz de-dupliokatora.
3.	Możliwość zarządzania procesem wyszukiwania danych backup'owych.
4.	Integracja z oferowanym rozwiązaniem dedykowanym do raportowania, możliwość inicjowania raportów.
Opis wdrożenia	
Lp.	**Zakres prac do wykonania**
1.	Instalacja virtualizatora na istniejącym serwerze backup.
2.	Instalacja maszyny wirtualnej de-duplikatora.
3.	Podstawowa konfiguracja interfejsów sieciowych, FQDN, NTP.
4.	Aktualizacja systemu operacyjnego do najnowszej wersji.
5.	Konfiguracja powiadomień SMTP/SNMP – zgodnie z wymaganiami Zamawiającego.
6.	Utworzenie systemu plików, konfiguracja protokołów szyfrowania i komunikacji – zgodnie z wymaganiami Zamawiającego.
7.	Utworzenie użytkowników de-duplikatora– zgodnie z wymaganiami Zamawiającego.
8.	Definicja integracji de-duplikatora z systemem backupu.
9.	Instalacja maszyny wirtualnej z systemem backupowym.
10.	Konfiguracja serwerów proxy.
11.	Konfiguracja datasetów.
12.	Instalacja agentów na systemach maszyn wirtualnych.
13.	Instalacja konsoli zarządzającej.
14.	konfiguracja powiadomień.
15.	Utworzenie (migracja z dotychczasowego systemu) zadań backupowych – zgodnie z wymaganiami Zamawiającego.
16.	Wykonanie kopii bezpieczeństwa maszyn wirtualnych.
17.	Wykonanie testowego odtworzenia maszyn wirtualnych.
18.	Weryfikacja poprawności działania odtworzonych maszyn – sprawdzenie integralności danych.
19.	Przeprowadzenie szkolenia w siedzibie Zamawiającego dla 4 administratorów – pracowników Wydziału Informatyki i Cyberbezpieczeństwa w oparciu o wdrożony, uruchomiony i przetestowany system.
20.	Po wykonaniu wdrożenia Wykonawca przekaże dokumentację techniczną powykonawczą, zawierającą minimum strukturę modelowanego systemu wraz z opisem technicznym funkcjonalności oraz zależności poszczególnych obiektów.

3.System do dystrybucji oprogramowania i aktualizacji wraz z wdrożeniem.

licencja wraz z minimum podstawowym rocznym wsparciem na zaoferowany produkt

Lp.	Cechy/minimalne wymagania
	Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia systemu do dystrybucji systemów operacyjnych, oprogramowania i aktualizacji dla systemów operacyjnych i innych oprogramowań oraz środowisk wspierających.
Ogólne wymagania dotyczące oferowanego oprogramowania	
1.	Oprogramowanie powinno spełniać standard budowy modułowej, z możliwością rozszerzenia o inne funkcjonalności i ich obsługę z poziomu konsoli zarządzającej.
2.	Oprogramowanie musi posiadać architekturę serwer-klient oraz konsolę zarządzającą nie tylko w wersji webowej.
3.	Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji administratora w konsoli zarządzającej, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej powinno być zintegrowane z kontami Active Directory.
4.	Oprogramowanie musi wspierać MsSQL-Server (również w wersji Express).
5.	Oprogramowanie musi posiadać Agenta dla systemów klienckich Windows oraz Windows Server.
6.	Oprogramowanie musi wspierać: • więcej niż jeden serwer-repozytorium (DIP-Server), • PXE-Relay, • WakeUp-Points, • integrację z Active Directory.
7.	Oprogramowanie musi posiadać system ról, dzięki któremu jest możliwe przypisywanie wybranych grup stanowisk do poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje grupowe obejmują wtedy tylko w/w przypisane grupy stanowisk.
8.	Oprogramowanie serwera aplikacji musi umożliwiać wysyłanie powiadomień mailowych.
9.	Oprogramowanie agenta musi realizować wszystkie wymagane funkcjonalności z poziomu jednej instancji usługi lub procesu bez wykorzystywania aplikacji oraz usług firm trzecich za wyjątkiem aplikacji oraz usług wbudowanych w system operacyjny na którym zainstalowany został agent.
10.	Oprogramowanie musi umożliwiać tworzenia zadań (Job-ów).
11.	Oprogramowania musi umożliwiać wyświetlenie informacji i stanu/statusów dostępnych w czasie rzeczywistym.
12.	Oprogramowanie musi posiadać wsparcie dla grup dynamicznych na potrzeby indywidualnych informacji/widoku.
13.	Dostarczone licencje na oprogramowanie muszą być bezterminowe.

Szczegóły dotyczące zadań (Job-ów).	
1.	Oprogramowanie musi umożliwiać wysyłanie polecenia w trybie: • "Push", • ”Pull”, • ”shutdown”.
2.	Oprogramowanie pozwala na indywidualną interakcję użytkownika w trakcie wykonywania zadania uruchomionego przez administratora w trybach: opóźnienie, odmowa, przypomnienie o instalacji.
3.	Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
4.	Zadania mogą być inicjowane z poziomu aplikacji selfservice - konsoli Webowej.
5.	Zawartość aplikacji SelfService (Kiosku) może być definiowana zarówno per User/Grupa Userów jak i per PC/Organisation Unit.
Szczegóły dotyczące możliwości instalacji systemów operacyjnych i sterowników.	
1.	Oprogramowanie musi posiadać wbudowany kreator dla instalacji i dystrybucji systemu operacyjnego.
2.	Oprogramowanie musi posiadać automatyczną integrację sterowników.
3.	Oprogramowanie musi posiadać funkcje plug & play. Po jednorazowym zapisie w bazie danych zestawu sterowników, oprogramowanie samodzielnie wykryje komponenty na podstawie oznaczeń PCI i wykona instalację dla każdego klienta zgodnie z wyposażeniem sprzętowym.
4.	Oprogramowanie musi posiadać możliwość integracji dodatkowych funkcji w zakresie tworzenia dodatkowych w trakcie instalacji systemu operacyjnego (instalacja patchy, oprogramowania, inwentaryzacja etc.).
5.	Oprogramowanie musi posiadać „Boot Client” i zintegrowany serwer PXE – dzięki czemu automatycznie wykrywane są nowe komputery i wprowadzane je do bazy danych. Funkcja „Boot Client” wprowadza sterowniki dla wszystkich kart sieciowych. Jeśli nie istnieje jeszcze profil oprogramowania, od razu definiowane jest oprogramowanie, które ma być później instalowane. Za pomocą „skanera sieci” oprogramowanie w połączeniu z Wake-On-LAN automatycznie instaluje nowe komputery. Oczywiście nadal jest możliwość korzystania z własnych profili sprzętowych.
6.	Oprogramowanie dla obrazów ISO Windows 10 musi umożliwiać ustawienie konfiguracji w obrazie, poprzez ich wyklikanie na etapie przygotowywania ISO, takich jak np: włączenie/wyłączenie funkcji telemetrii i Cortany, możliwość dołączenia od razu wybranych patchy, aplikacji itp.
Szczegóły dotyczące możliwości instalacji innych oprogramowań.	
1.	Oprogramowanie musi posiadać kreator do tworzenia pakietów, w skład których wchodzi różnorodne oprogramowanie.
2.	Oprogramowanie musi umożliwiać detekcję oraz wsparcie kreatora dla wielu mechanizmów instalacji: MSI, InnoSetup, NullSoft, Wise-Installer i inne.
3.	Oprogramowanie musi umożliwiać uzupełnienie instalacji oprogramowania na urządzeniu końcowym o dodatkowe kroki ze strony użytkownika końcowego (np.: deaktywacja okna powitalnego, itp).
4.	Oprogramowanie musi integrować procedurę odinstalowania.
5.	Oprogramowanie musi umożliwiać natywną instalację pakietów (a nie tylko wrap aplikacji w innym skrypcie instalacyjnym) oraz transparentną (w Logach znajduje się informacja dotycząca instalacji np.: msiexec.exe /i \\...\software-xyz.msi /qn /noreboot).

6.	Oprogramowanie musi umożliwiać indywidualna konfigurację zależności (np.: .uprzednia instalacja .net (w przypadku jeśli takowa nie miała jeszcze miejsca), następnie instalacja docelowego oprogramowania), a także ustawianie zachowań w trakcie Reboot również dla oprogramowania.
7.	Oprogramowanie musi wprowadzać możliwość użycia własnych skryptów , żeby np.: customizować linki, rejestry, Working Directories, itd.
8.	Wymaga się narzędzia do nagrywania kroków instalacji oprogramowania, tak, by administrator mógł przejść wszystkie kroki instalatora i wypchnąć tak wyklikany instalator zdalne.
9.	Oprogramowanie musi oferować funkcję różnorodnej weryfikacji instalacji (np.: jaka jest wartość zwrotna programu instalacyjnego, czy istnieje jakiś określony wpis do rejestru lub usługa).
10.	Oprogramowanie musi umożliwiać ustawienie dowolnego kontekstu security/uprawnień z jakimi dana paczka ma zostać zainstalowana na urządzeniu końcowym.
Wymagania dotyczące dystrybucji poprawek dla systemów operacyjnych.	
1.	Oprogramowanie musi umożliwiać dystrybucję patchy Windows bez WSUS oraz triggerowanie z poziomu WSUS.
2.	Oprogramowanie musi umożliwiać obsługę systemów operacyjne Microsoft —Windows Server 2008R2, Windows Server 2012, 2016, Windows Server 2019 z natywną instalacją.
3.	Producent oprogramowania musi zapewniać stały dostęp do bazy danych z poprawkami Microsoft – baza jest dostępna dla Klienta z poziomu konsoli oprogramowania w dniu jej opublikowania przez Microsoft.
4.	Oprogramowanie musi umożliwiać określenie ścisłych wymagań czasowych dla instalacji poprawek Microsoft i te wymagania kontrolować. Oprogramowanie nie wymaga ingerencji w reguły eksploatacji serwerów, a mimo to zapewnia ich odpowiednio szybkie zamknięcie w razie luk w zabezpieczeniach.
5.	Oprogramowanie musi pozwalać administratorowi zarządzać aktualizacją systemów: możliwość sprawdzania tylko pod kątem brakujących poprawek i czy poprawki mają być od razu instalowane. Poprawki mogą być zatwierdzane automatycznie lub ręcznie. Oprogramowanie pozwala także ustalać reguły dla różnych grup w systemie IT.
6.	Oprogramowania musi pozwalać by metodą drag and drop w środowisku zgodnym z MMC określać, w jakich systemach mają być instalowane poprawki. W taki sam sposób definiowane są również automatyczne instalacje i sytuacje, w których administrator ma być wcześniej pytany o zgodę. Oprogramowanie automatycznie pobiera wszystkie poprawki Microsoft i na żądanie automatycznie je rozprowadza w infrastrukturze Klienta zgodnie z wytycznymi administratora.
Szczegóły oprogramowania dotyczące kreatora skryptów, konfiguracji pakietów i automatyzacji procesów.	
1.	Oprogramowanie musi pozwalać na tworzenie plików transformacji (MST), które umożliwiają niezawodne dopasowanie do każdego MSI.
2.	Oprogramowanie musi pozwalać na tworzenie kreatora instalacji dla dowolnej aplikacji – nie wymaga paczki MSI.
3.	Oprogramowanie musi pozwalać tworzyć pakiety instalacyjne, gdzie w ramach procesu można zainstalować "n" aplikacji lub wykonać szereg dodatkowych funkcji związanych np. z inwentaryzacja.

4.	Oprogramowanie musi obsługiwać wszystkie powszechnie dostępne na rynku systemy operacyjne Microsoft: Windows10, Windows Server 2008R2, Windows Server 2012, 2016 i Windows Server 2019.
5.	Oprogramowanie musi umożliwiać tworzenie plików sterujących (tansform).
6.	Oprogramowanie musi pozwalać na automatyzacje niemal każdego procesu wykonywanego ręcznie na komputerze.
7.	Oprogramowania musi pozwalać na proste tworzenie skryptów metodą drag and drop.
8.	Oprogramowanie musi zawierać standardowy zestaw poleceń.
9.	Oprogramowanie musi posiadać możliwość sterowania również interfejsami niezgodnymi ze standardem (np. Java).
10.	Oprogramowanie musi posiadać pomoc kontekstową.
11.	Oprogramowanie musi posiadać tryb testowy step by step.
Ogólna uwaga dotycząca wdrożenia.	
1.	Wdrożenie polegać będzie w szczególności na: • zainstalowaniu i uruchomieniu środowiska systemu, jego konfiguracji wg. potrzeb Zamawiającego na wskazanym serwerze, • integracji z Active Directory, • zestawieniu komunikacji pomiędzy stacjami roboczymi oraz serwerami, • dystrybucji agentów, • utworzeniu polityk oraz konfiguracji tak aby wyeliminować usługę WSUS, • przetestowaniu pozostałych funkcjonalności dotyczących dystrybucji systemów i oprogramowań. Pozostałe szczegóły dotyczące wdrożenia zostaną określone przez pracowników Wydziału Informatyki i Cyberbezpieczeństwa w zależności od zaproponowanego rozwiązania na etapie realizacji.
2.	Wykonawca przeprowadzi szkolenie w siedzibie Zamawiającego dla 4 administratorów – pracowników Wydziału Informatyki i Cyberbezpieczeństwa w oparciu o wdrożony, uruchomiony i przetestowany system.
3.	Po wykonaniu wdrożenia Wykonawca przekaże dokumentację techniczną powykonawczą, zawierającą minimum strukturę modelowanego systemu wraz z opisem technicznym funkcjonalności oraz zależności poszczególnych obiektów.