Załącznik do Formularza ofertowego
Nr ORG.14.1.2025. AR z dnia 30 kwietnia 2025 roku
- szczegółowy wykaz oferowanego sprzętu i rozwiązań

DT* - udokumentowanie wymogu/specyfikacji

ROZWÓJ SYSTEMU ANTYWIRUSOWEGO / PODNIESIENIE WERSJI OPROGRAMOWANIA DO WYŻSZEJ Z OPROGRAMOWANIEM XDR		
PRODUCENT, NAZWA ROZWIĄZANIA	DT*	***Podać nazwę producenta oraz nazwę rozwiązania***
Podstawowe informacje:		
Istniejący system ochrony urządzeń ESET należy rozbudować w zakresie modułu posiadającego narzędzia wykrywania incydentów i automatycznego reagowania umożliwiającego korelację zdarzeń (XDR), mechanizmy uwierzytelniania wieloskładnikowego (MFA) oraz w zakresie proaktywnej ochrony przed zagrożeniami zero-day z analizą w odizolowanym chmurowymśrodowisku. Nr licencji obecnie posiadanego systemu: 3AA-884-A57		*Opisać oferowane parametry*
W wyniku rozbudowy systemu o nowe moduły funkcjonalne przy zachowaniu dotychczasowej funkcjonalności w zakresie ochrony stacji roboczych, ochrony serwerów, ochrony urządzeń mobilnych. Nowe moduły muszą być kompatybilne z istniejącym systemem, a całe rozwiązanie musi zapewniać minimum funkcjonalność określoną w punktach poniżej.		*Opisać oferowane parametry*
Zamawiający dopuszcza zastosowanie rozwiązania równoważnego pod warunkiem realizowania wszystkich wymaganych funkcjonalności. Zastosowanie rozwiązania równoważnego obliguje Wykonawcę do złożenia dokumentacji potwierdzającej, iż zaproponowane rozwiązanie wymagania funkcjonalne – m.in. wyniki porównań, testy.		*Opisać jeżeli dotyczy*
Dostarczenie rozwiązania równoważnego musi przebiec w sposób niezakłócający bieżącej pracy Zamawiającego. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników,		*Opisać oferowane parametry*

skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania Oprogramowania w środowisku		
Wymagania:		
Nowe moduły muszą być kompatybilne z istniejącym rozwiązaniem oraz muszą być zarządzane z jednej centralnej konsoli administracyjnej dostępnej z poziomu interfejsu WWW zabezpieczonego protokołem SSL.		*Opisać oferowane parametry*
Konsola administracyjna musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.		*Opisać oferowane parametry*
Moduł XDR musi być oparty o motor baz danych SQL celem zapewnienia maksymalnej wydajności pracy i maksymalnej ochrony danych. Motor bazy SQL należy dostarczyć wraz z modułem XDR		*Opisać oferowane parametry*
Wymagana ilość licencji na nowe moduły: minimum 26 szt.		*Opisać oferowane parametry*
***Funkcjonalność XDR*:**		
Automatyczna wizualizacja zdarzeń, incydentów i ataków ukierunkowanych		*Opisać oferowane parametry*
Możliwość wyszukiwania zagrożeń na podstawie definiowanych filtrów		*Opisać oferowane parametry*
Wbudowany zestaw reguł zapewniający reagowanie na wykryte incydenty z możliwością budowania własnych reguł oraz edycji istniejących		*Opisać oferowane parametry*
Możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.		*Opisać oferowane parametry*
Możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa		*Opisać oferowane parametry*
Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.		*Opisać oferowane parametry*
Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika		*Opisać oferowane parametry*
Możliwość uruchomienia reguł w oparciu o dane historyczne.		*Opisać oferowane parametry*
Możliwość blokowania plików po sumach kontrolnych.		*Opisać oferowane parametry*
Możliwość ustawiania priorytetu zdarzeń		*Opisać oferowane parametry*

Możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku		*Opisać oferowane parametry*
Możliwość oznaczenia plików DLL jako bezpieczne, pobrania do analizy oraz ich zablokowania.		*Opisać oferowane parametry*
Weryfikacja uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia.		*Opisać oferowane parametry*
Dla wykonanego skryptu lub pliku exe, weryfikacja powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.		*Opisać oferowane parametry*
Możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal).		*Opisać oferowane parametry*
Możliwość włączenia izolacji komputera od sieci.		*Opisać oferowane parametry*
Funkcjonalność MFA:		
Wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.		*Opisać oferowane parametry*
Możliwość integracji minimum z systemem operacyjnym Windows Server poprzez konsolę zarządzającą systemu operacyjnego.		*Opisać oferowane parametry*
Moduł zarządzania uwierzytelnianiem się użytkowników musi integrować się minimum z wbudowanym w systemie operacyjnym Windows Server modułem do zarządzania kontami użytkowników w postaci dodatkowej zakładki we właściwościach użytkownika.		*Opisać oferowane parametry*
Możliwość określenia metody uwierzytelniania dwuskładnikowego użytkowników, minimum wiadomość SMS, aplikacja mobilna		*Opisać oferowane parametry*
Do wysyłania wiadomości SMS nie może być wymagane posiadanie własnej bramy SMS i centrali GSM. Wysyłanie wiadomości SMS z hasłami jednorazowymi musi odbywać się z infrastruktury producenta rozwiązania.		*Opisać oferowane parametry*
Możliwość wysyłania wiadomości na telefony pracujące w roamingu.		*Opisać oferowane parametry*
Możliwość wyboru użytkowników uwierzytelniania dwuskładnikowego.		*Opisać oferowane parametry*

Możliwość ograniczenia dostępu przy uwierzytelnianiu metodą RADIUS do grupy		*Opisać oferowane parametry*
użytkowników wskazanych w konfiguracji.		*Opisać oferowane parametry*
Rozwiązanie musi posiadać mechanizm zabezpieczający przed atakiem typu brute-force, które po określonej liczbie prób nieudanego logowania musi automatycznie zablokować możliwość uwierzytelnienia się dla danego użytkownika.		*Opisać oferowane parametry*
W ramach modułu musi być zapewniony dostęp do dedykowanej aplikacji mobilnej działającej pod kontrolą Android i iOS		*Opisać oferowane parametry*
Dostępne API pozwalające programistom na zintegrowanie rozwiązania z serwisem web lub oprogramowaniem wykorzystującym uwierzytelnianie w oparciu minimum o usługę Active Directory. Dla środowisk nie wykorzystujących usług Active Directory musi być dostępny pakiet SDK umożliwiający implementację w tych środowiskach, dwuskładnikowego uwierzytelniania do autoryzacji użytkowników.		*Opisać oferowane parametry*
Funkcjonalność Sandboxingu w chmurze:		
Wbudowany serwer RADIUS umożliwiający uwierzytelnia-nie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.		*Opisać oferowane parametry*
Możliwość integracji minimum z systemem operacyjnym Windows Server poprzez konsolę zarządzającą systemu operacyjnego.		*Opisać oferowane parametry*
Moduł zarządzania uwierzytelnianiem się użytkowników musi integrować się minimum z wbudowanym w systemie operacyjnym Windows Server modułem do zarządzania kontami użytkowników w postaci dodatkowej zakładki we właściwościach użytkownika.		*Opisać oferowane parametry*
Ochrona przed zagrożeniami 0-day.		*Opisać oferowane parametry*
Możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.		*Opisać oferowane parametry*
Możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.		*Opisać oferowane parametry*
Możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.		*Opisać oferowane parametry*
Tworzenie listy wykluczeń określonych plików lub folderów z przesyłania.		*Opisać oferowane parametry*

Możliwość wyświetlenia listy plików, które zostały przesłane do analizy.		*Opisać oferowane parametry*
Możliwość analizowania plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.		*Opisać oferowane parametry*
Funkcjonalność ochrony stacji roboczych:		
Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.		*Opisać oferowane parametry*
Ochrona przed rootkitami oraz podłączeniem komputera do sieci botnet.		*Opisać oferowane parametry*
Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.		*Opisać oferowane parametry*
Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.		*Opisać oferowane parametry*
Skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.		*Opisać oferowane parametry*
Skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.		*Opisać oferowane parametry*
Umieszczenia na liście wykluczeń wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.		*Opisać oferowane parametry*
Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).		*Opisać oferowane parametry*
Skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.		*Opisać oferowane parametry*
Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.		*Opisać oferowane parametry*
Blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, optycznych pamięci masowych, pamięci masowych firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth,		*Opisać oferowane parametry*

czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.		
Blokowanie nośników wymiennych, bądź grup urządzeń wraz z możliwością tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.		*Opisać oferowane parametry*
Możliwość generowania raportu dotyczącego stacji, zawierającego informacje dotyczące, minimum: zainstalowanych aplikacji, usług systemowych, systemu operacyjnego, aktywnych procesów, połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.		*Opisać oferowane parametry*
Automatyczna, inkrementalna aktualizacja silnika detekcji.		*Opisać oferowane parametry*
Tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).		*Opisać oferowane parametry*
Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.		*Opisać oferowane parametry*
Zintegrowany moduł bezpiecznej przeglądarki. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez użytkownika.		*Opisać oferowane parametry*
Zintegrowany moduł kontroli dostępu do stron internetowych.		*Opisać oferowane parametry*
Możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.		*Opisać oferowane parametry*
Ochrona przed zagrożeniami 0-day.		*Opisać oferowane parametry*
Funkcjonalność ochrony serwerów:		
Ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.		*Opisać oferowane parametry*
Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.		*Opisać oferowane parametry*
Skanowania dysków sieciowych typu NAS.		*Opisać oferowane parametry*
Wbudowane minimum dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.		*Opisać oferowane parametry*
Automatyczna, inkrementalna aktualizacja silnika detekcji.		*Opisać oferowane parametry*
Możliwość wykluczania ze skanowania procesów.		*Opisać oferowane parametry*

Możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.		*Opisać oferowane parametry*
System zapobiegania włamaniom działający na hoście (HIPS).		*Opisać oferowane parametry*
Skanowanie magazynu Hyper-V.		*Opisać oferowane parametry*
Skaner UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.		*Opisać oferowane parametry*
Możliwość blokowania zewnętrznych nośników danych na serwerze w tym przynajmniej: pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.		*Opisać oferowane parametry*
Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.		*Opisać oferowane parametry*
Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.		*Opisać oferowane parametry*
Ochrona przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.		*Opisać oferowane parametry*
Możliwość uruchomienia lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.		*Opisać oferowane parametry*
Funkcjonalność ochrony urządzeń mobilnych:		
Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.		*Opisać oferowane parametry*
Automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).		*Opisać oferowane parametry*
Możliwość skonfigurowania zaufanej karty SIM.		*Opisać oferowane parametry*
Wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi usunięcie zawartości urządzenia, przywrócenie urządzenie do ustawień fabrycznych, zablokowania urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS.		*Opisać oferowane parametry*
Wyświetlenie listy zainstalowanych aplikacji.		*Opisać oferowane parametry*

Blokowanie aplikacji w oparciu o nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła.		*Opisać oferowane parametry*
Skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.		*Opisać oferowane parametry*
ZAKUP OPROGRAMOWANIA DLP		
PRODUCENT, NAZWA ROZWIĄZANIA	DT*	***Podać nazwę producenta oraz nazwę rozwiązania***
Wymagania:		
Wsparcie instalacji w oparciu o bazę MS SQL.		*Opisać oferowane parametry*
Praca w architekturze serwer, agent, klienta gdzie komunikacja serwera zarządzającego z klientem odbywa się tylko przy pomocy agenta.		*Opisać oferowane parametry*
Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.		*Opisać oferowane parametry*
Rozwiązanie musi być dostępne minimum w polskiej wersji językowej.		*Opisać oferowane parametry*
Możliwość aktualizacji komponentów własnych.		*Opisać oferowane parametry*
Automatyczne pobieranie aktualizacji definicji kategoryzowania stron internetowych oraz aplikacji. Musi być możliwość wyłączenia automatycznego pobierania.		*Opisać oferowane parametry*
Rozwiązanie musi uwzględniać 26 użytkowników/stacji roboczych. Jeżeli wymagana jest licencja obejmująca ilość użytkowników lub stacji roboczych należy ja dostarczyć.		*Opisać oferowane parametry*
Funkcjonalność:		
Wymuszenie komunikacji w czasie rzeczywistym dla wybranej stacji komputerowej w celu sprawdzania konfiguracji.		*Opisać oferowane parametry*
Możliwość zablokowania/uruchomienia trybu awaryjnego na stacji końcowej		*Opisać oferowane parametry*
Możliwość ustawień powiadomień dla użytkownika końcowego w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP.		*Opisać oferowane parametry*
Możliwość audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, dokumenty		*Opisać oferowane parametry*

drukowane, ruch sieciowy, wysyłane oraz odbierane wiadomości e-mail oraz wykonywane czynności na plikach.		
Filtrowanie poprzez podanie zakresu czasu.		*Opisać oferowane parametry*
Analiza lub tagowanie nowo powstałych plików wrażliwych w oparciu o minimum: a) aplikację z której zostały utworzone b) lokalizację lokalną oraz sieciową c) adres URL, z którego został pobrany plik d) format pliku e) zawartość pliku		*Opisać oferowane parametry*
Analiza lub tagowania posiadanych plików wrażliwych w oparciu o minimum: lokalizację lokalną oraz sieciową, format pliku oraz zawartość pliku.		*Opisać oferowane parametry*
Dla tagowanych plików możliwość utworzenia reguł w oparciu o czynności: a) blokowania oraz zezwalania na zapisywanie, przenoszenie plików do lokalizacji na dyskach lokalnych lub konfiguracji określonych lokalizacji, do której będzie możliwość bądź nie będzie możliwości zapisu. b) blokowania oraz zezwalania na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń. c) zabezpieczenia możliwości drukowania, utworzenia białej oraz czarnej listy drukarek. d) blokowania oraz zezwalania na zapisywanie, przenoszenie do lokalizacji sieciowej oraz określenie białej oraz czarnej listy lokalizacji sieciowych. e) blokowania oraz zezwalania wysyłki plików za pośrednictwem klientów pocztowych oraz określenia białej oraz czarnej listy adresów e-mail oraz domen. f) blokowania oraz zezwalania na zapisywanie, przenoszenie plików na dyski zaszyfrowane w oparciu o lokalnie zaszyfrowane dyski oraz zewnętrzne zaszyfrowane dyski.		*Opisać oferowane parametry*

g) blokowania oraz zezwalania na zapisywanie, przenoszenie plików do folderów synchronizacji z usługami chmury (Google Drive, OneDrive Business, One Drive Personal, Dropbox, Box Sync, SharePoint). h) blokowania oraz zezwalania na zapisywanie, przenoszenie plików poprzez usługę pulpitu zdalnego i) blokowania oraz zezwalania na wykonywanie zrzutów ekranowych, skopiowania zawartości, nagrywania na płyty CD/DVD oraz wirtualnego drukowania plików. j) uruchomienia wybranego formatu pliku przez wskazaną przez administratora aplikacje.		
Możliwość określenia stref urządzeń pamięci masowej		*Opisać oferowane parametry*
Możliwość globalnego zablokowania oraz zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury (Google Drive, OneDrive Business, One Drive Personal, Dropbox, Box Sync, SharePoint).		*Opisać oferowane parametry*
Szyfrowanie dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzowanie do zaszyfrowanych nośników wymiennych musi być w pełni niezauważalne dla użytkownika.		*Opisać oferowane parametry*
Możliwość tworzenia kluczy szyfrujących które będą kompatybilne z funkcjonalnością BitLocker dla zapewnienia transparentności współdzielenia zaszyfrowanych nośników wymiennych.		*Opisać oferowane parametry*
Możliwość globalnego zablokowania, zezwolenia, dostępu tylko do odczytu z korzystania z określonych urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.		*Opisać oferowane parametry*
Możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.		*Opisać oferowane parametry*
Możliwość wygenerowania hasła ratunkowego do odblokowania dostępu do zaszyfrowanych dysków oraz dysków wymiennych, w sytuacji jeżeli użytkownik zapomni hasła.		*Opisać oferowane parametry*

Blokowanie stron internetowych w oparciu o kategorię stron oraz po podaniu adresu URL. Musi istnieć możliwość konfiguracji przekierowania z dowolnej strony która została zablokowana.		*Opisać oferowane parametry*
Możliwość określenia stref urządzeń pamięci masowej.		*Opisać oferowane parametry*
Raportowanie:		
Możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, dokumenty drukowane, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.		*Opisać oferowane parametry*
Możliwość raportowania reguł bezpieczeństwa w oparciu o incydenty na plikach chronionych, ogółu wykonanych operacji na plikach, podsumowania wszystkich incydentów bezpieczeństwa, akcji użytkowników na zabezpieczonych plikach, zablokowanych operacji na dyskach lokalnych, zewnętrznych, podsumowanie korzystania z urządzeń oraz ich typów.		*Opisać oferowane parametry*
Możliwość utworzenia raportu w oparciu o użycie aplikacji, zablokowanych aplikacji, zablokowanych drukarek, podsumowanie drukowania, zablokowane strony internetowe, zablokowanych użytkowników, aktywność użytkowników na serwerze, alarmy, ustawień klienta, kopii bezpieczeństwa, zarządzania stacjami końcowymi, dezaktywacją licencji oraz zaawansowanego debugowania.		*Opisać oferowane parametry*
Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.		*Opisać oferowane parametry*
Raporty muszą być generowane do pliku PDF, XLS po podaniu lokalizacji zapisywanego pliku, na wskazane adresy e-mail.		*Opisać oferowane parametry*
Administracja:		
Synchronizacja użytkowników oraz stacji roboczych z usługą Active Directory.		*Opisać oferowane parametry*
Możliwość zarządzania bazą danych poprzez określone zadania – kopii bazy danych, kopii oraz usunięcia bazy danych, usunięcia bazy danych, ustawieniach kopii bazy danych - dostępne z poziomu konsoli wraz z określeniem		*Opisać oferowane parametry*

automatycznego powtarzania zadań: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.		
Możliwość zdefiniowania przedziału czasowego dla kopii zapasowej bazy programu.		*Opisać oferowane parametry*
Funkcje automatycznej kopii bazy danych programu DLP co 7, 14, 30 dni		*Opisać oferowane parametry*
Tworzenie nowych/usuwanie/klonowanie kont administratorów w konsoli programu.		*Opisać oferowane parametry*
Możliwość zmiany hasła oraz loginu innego administratora.		*Opisać oferowane parametry*
Przypisywanie / odbieranie uprawnień do wybranych modułów programu.		*Opisać oferowane parametry*
Możliwość logowania za pośrednictwem grup domenowych administratorów.		*Opisać oferowane parametry*
Możliwość ustawienia godzin w których nie będą obowiązywały użytkowników reguły kontroli aplikacji oraz stron internetowych. Godziny pracy muszą być ustalane dla poszczególnych dni tygodnia.		*Opisać oferowane parametry*
Możliwość określenia czy dokumenty zawierające dane wrażliwe takie jak numery Kart kredytowych, numer PESEL, numer polskiego dowodu osobistego, wyrażenia regularne, określone ciągi znaków, numer IBAN, mogą zostać przesłane do chmur lub innych źródeł WWW.		*Opisać oferowane parametry*
Określanie bezpiecznych stref oraz domen do których pliki mogą zostać przesłane.		*Opisać oferowane parametry*
Możliwość określenia czy dokumenty zawierające dane wrażliwe takie jak numery Kart kredytowych, numer PESEL, numer polskiego dowodu osobistego, wyrażenia regularne, określone ciągi znaków, numer IBAN, mogą zostać przesłane na urządzenia zewnętrzne.		*Opisać oferowane parametry*
Możliwość przygotowania pliku instalacyjnego agenta.		*Opisać oferowane parametry*
Możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.		*Opisać oferowane parametry*
Konsola zdalna:		

Możliwość przeglądania informacji dotyczących bezpieczeństwa w oparciu o próby wycieku danych, operacji na plikach posiadających tag, plików wysyłanych do sieci, plików pobieranych z sieci, plików wysyłanych drogą e-mailową, plików kopiowanych na dyski zewnętrzne, pliki drukowane. Konsola webowa musi umożliwiać obserwację produktywności pracy użytkowników w oparciu o zdefiniowane przez administratora aplikacje oraz strony internetowe.		*Opisać oferowane parametry*
Możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.		*Opisać oferowane parametry*
Możliwość instalacji na systemach Windows Server 2008 R2 lub nowszych.		*Opisać oferowane parametry*
Możliwość współdziałania z bazą danych MS SQL Server 2012 i nowszymi.		*Opisać oferowane parametry*
Logowanie do konsoli webowej musi opierać się na wcześniej utworzonych kontach użytkowników w konsoli aplikacyjnej.		*Opisać oferowane parametry*
Uprawnienia dostępu wybranych użytkowników do poszczególnych informacji na temat grup komputerów lub grupy użytkowników w konsoli webowej, muszą być ustalane z poziomu konsoli aplikacyjnej.		*Opisać oferowane parametry*
Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na: a) Bezpieczeństwo danych: – przegląd informacji o incydentach bezpieczeństwa. – przegląd danych przychodzących. – przegląd danych wychodzących. – przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików. – podłączane/odłączane urządzenia przenośne. b) Produktywność: – przegląd informacji na temat produktywności użytkowników.		*Opisać oferowane parametry*

– aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji. – trendy c) Eksploatacja sprzętu: – przegląd informacji na temat eksploatacji sprzętu komputerowego. – eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery. – eksploatacja drukarek. – eksploatacji sieci.		
Możliwość dodania klucza licencji.		*Opisać oferowane parametry*
Możliwość konfiguracji/zmiany domyślnego serwera SMTP.		*Opisać oferowane parametry*
Weryfikacja wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.		*Opisać oferowane parametry*
Generowanie raportów z danymi na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu. Raporty muszą być generowane dla wybranych grup komputerów/użytkowników w interwałach tygodniowych lub miesięcznych. Raporty będą przesyłane drogą e-mailową.		*Opisać oferowane parametry*
ZAKUP SERWERÓW WRAZ Z OPROGRAMOWANIEM		
PRODUCENT, MODEL, ROK PRODUKCJI (2024 lub 2025)	DT*	***Podać nazwę producenta, model oraz rok produkcji***
Obudowa:		
Obudowa typu RACK o wysokości maksymalnej 2U		*Opisać oferowane parametry*
Możliwość instalacji min. 8 dysków 2,5” Hot-Plug	DT	*Opisać oferowane parametry*
Obudowa wyposażona w panel diagnostyczny lub sygnalizację LED umieszczoną na froncie obudowy informująca o stanie procesora, pamięci, dyskach, temperaturze.	DT	*Opisać oferowane parametry*

Przedni panel bądź ramka zamykana na klucz, chroniąca dyski przed nieuprawnionym wyjęciem.	DT	*Opisać oferowane parametry*
Płyta główna:		
Płyta główna z możliwością zainstalowania minimum dwóch procesorów	DT	*Opisać oferowane parametry*
Możliwość obsługi minimum 6 TB RAM.	DT	*Opisać oferowane parametry*
Zintegrowany z płytą główną moduł TPM2.0	DT	*Opisać oferowane parametry*
Minimum 2 sloty PCIe generacji 5, w tym slot x16 pełnej wysokości (full height)	DT	*Opisać oferowane parametry*
Procesor:		
Dwa procesory wielordzeniowe osiągające w teście PassMark CPU Mark wynik min. 38.000 pkt według danych ze strony https://www.cpubenchmark.net/cpu_list.php dla konfiguracji wieloprocesorowej		*Opisać oferowane parametry*
Pamięć RAM:		
Zainstalowana pamięć RAM minimum 256 GB RDIMM DDR5.		*Opisać oferowane parametry*
Możliwe zabezpieczenia pamięci, minimum: ECC, SDDC lub równoważne, Rank Sparing lub równoważne		*Opisać oferowane parametry*
Pamięć masowa:		
Zainstalowane dwa dyski 1,92 TB SSD w RAID1,		*Opisać oferowane parametry*
Możliwość instalacji dysków twardych SATA, SAS, SSD, M.2	DT	*Opisać oferowane parametry*
Kontroler:		
Sprzętowy kontroler dyskowy RAID minimum 4GB cache zapewniający obsługę zainstalowanych napędów dyskowych oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60.	DT	*Opisać oferowane parametry*
Pamięć cache podtrzymywana bateryjne lub za pomocą pamięci nieulotnej (NV RAM).		*Opisać oferowane parametry*
Karta graficzna:		
Zintegrowana karta graficzna o rozdzielczości minimum 1920x1200	DT	*Opisać oferowane parametry*
Wbudowane porty:		
Minimum 4 porty USB w tym co najmniej dwa w wersji 3.0 lub nowszej.	DT	*Opisać oferowane parametry*

Minimum 1 port video.	DT	*Opisać oferowane parametry*
Porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń. Zamawiający dopuszcza w serwerach stosowanie dodatkowych portów z wykorzystaniem certyfikowanych modułów rozszerzeń obudowy pod warunkiem ich dostarczenia. Porty nie mogą zostać osiągnięte poprzez zewnętrzne adaptery i przejściówki, nie mogą również zajmować slotów kart rozszerzeń PCI-E oraz wnęk na dyski.		*Opisać oferowane parametry*
Interfejsy sieciowe:		
Minimum jeden interfejs sieciowy 1 Gb Ethernet Base-T	DT	*Opisać oferowane parametry*
Minimum dwa interfejsy sieciowe 10 GbE SFP+		*Opisać oferowane parametry*
Jeden interfejs 1Gb w standardzie Base-T do zarządzania serwerem.	DT	*Opisać oferowane parametry*
Zasilanie:		
Redundantne zasilacze Hot Plug, każdy o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia o sprawności minimum 92% każdy przy 50% obciążeniu, pracujące w sieci 230V 50/60Hz prądu zmiennego		*Opisać oferowane parametry*
Wentylatory:		
Redundantne wentylatory typu Hot-Plug.		*Opisać oferowane parametry*
Zarządzanie:		
Moduł umożliwiający zdalne zarządzanie serwerem.	DT	*Opisać oferowane parametry*
Oprogramowanie do zdalnego zarządzania serwerem z licencją nie ograniczoną czasowo, zapewniające minimum: monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.), monitorowanie w czasie rzeczywistym poboru prądu przez serwer, zbieranie logów błędów hardware, przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury, montowanie wirtualnych napędów, zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego, wysyłanie zawiadomień droga mailową lub poprzez SNMP.		*Opisać oferowane parametry*
System operacyjny:		

Serwerowy system operacyjny Microsoft Windows Server 2025 lub równoważny		*Opisać oferowane parametry*
Licencja serwerowego systemu operacyjnego musi uwzględniać wszystkie rdzenie procesorów zainstalowanych w serwerze.		*Opisać oferowane parametry*
Licencja serwerowego systemu operacyjnego musi uprawniać do uruchamiania co najmniej czterech serwerowych systemów operacyjnych w środowisku wirtualnym.		*Opisać oferowane parametry*
Wraz z serwerowym systemem operacyjnym należy dostarczyć 30 licencji (dotyczy łącznej ilość wymaganych licencji dostarczonych z serwerami) dostępowych dające użytkownikom prawo korzystania z usług udostępnianych przez serwer oraz umożliwiające korzystanie z jego zasobów.		*Opisać oferowane parametry*
Licencje serwerowego systemu operacyjnego nie mogą być ograniczone czasowo.		*Opisać oferowane parametry*
Nie dopuszcza się licencji typu refurbished.		*Opisać oferowane parametry*
Certyfikaty i deklaracje:		
Deklaracja zgodności UE (Certyfikat CE). Urządzenie musi posiadać oznakowanie CE.		*Opisać oferowane parametry*
Certyfikat zgodności z dyrektywą RoHS lub dokument wystawiony przez niezależną, akredytowaną jednostkę potwierdzający spełnienie kryteriów środowiskowych zgodnych z dyrektywą RoHS o eliminacji substancji niebezpiecznych.		*Opisać oferowane parametry*
Deklaracja zgodności z dyrektywą WEEE lub oświadczenie producenta o spełnieniu obowiązków w zakresie postępowania z odpadami WEEE i zgodności z Ustawą z 11 września 2015 o zużytym sprzęcie elektrycznym i elektronicznym (Dz.U. 2024 poz.573). Urządzenie musi być oznaczone etykietą WEEE.		*Opisać oferowane parametry*
Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 lub równoważną oraz ISO-14001 lub równoważną.		*Opisać oferowane parametry*
ROZWÓJ SYSTEMU UTM ZE WSPARCIEM		
PRODUCENT, NAZWA ROZWIĄZANIA	DT*	***Podać nazwę producenta oraz nazwę rozwiązania***

Zamawiający obecnie używa zapory sieciowej Stormshield SN310 A42JP657A7 wraz z modułem pasywnego skanera badającego podatności sieci. Należy rozbudować istniejące rozwiązanie w zakresie dodatkowej funkcjonalności obejmującej rozbudowę filtra URL o dodatkowe kategorie tematyczne i analizę nieznanych plików w wyizolowanym, wirtualnym środowisku.		*Opisać oferowane parametry*
Filtr stron WWW:		
Wbudowany filtr URL oparty o technologię w chmurze, obsługujący minimum 54 kategorii z możliwością tworzenia własnych kategorii.		*Opisać oferowane parametry*
Filtr URL musi mieć możliwość korzystania z adresów WWW dostępnych w chmurze.		*Opisać oferowane parametry*
Musi udostępniać kategorie minimum spam, hacking, malwere, botnets.		*Opisać oferowane parametry*
Baza filtra WWW musi umożliwiać grupowanie w kategorie tematyczne.		*Opisać oferowane parametry*
Filtrowanie treści oraz szkodliwego oprogramowania w obrębie protokołów HTTP i HTTPS.		*Opisać oferowane parametry*
Możliwość blokowania i wysyłania treści poprzez HTTP i HTTPS.		*Opisać oferowane parametry*
Inspekcja z obsługą protokołu TLS 1.3.		*Opisać oferowane parametry*
Filtrowanie plików na podstawie MIME.		*Opisać oferowane parametry*
Analiza nieznanych plików:		
Detekcja złośliwych plików poprzez wykrywanie ataków oraz zagrożeń, realizowane poza siecią firmową, w odrębnym i bezpiecznym środowisku.		*Opisać oferowane parametry*
Ochrona przed zagrożeniami ukierunkowanymi oraz ransomware.		*Opisać oferowane parametry*
Inspekcja plików wykonywalnych np., .exe		*Opisać oferowane parametry*
Inspekcja plików dokumentów w tym .doc, .docx, .rtf		*Opisać oferowane parametry*
Inspekcja plików .pdf		*Opisać oferowane parametry*
Inspekcję plików archiwów w tym zip, arj, lha, rar, cab		*Opisać oferowane parametry*

Dynamiczna analiza behawioralna kodu uruchamianego w realnych środowiskach testowych Windows.		*Opisać oferowane parametry*
NAPĘD DYSKOWY RDX **NOŚNIK DANYCH**		
PRODUCENT, MODEL	DT*	***Podać nazwę producenta oraz nazwę rozwiązania***
Obudowa:		
Obudowa typu TOWER		*Opisać oferowane parametry*
Wyposażona w minimum dwie kieszenie wymienne dyski 2,5” lub 3,5”		*Opisać oferowane parametry*
Zasilanie:		
zasilacz o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujący w sieci 230V 50/60Hz prądu zmiennego		*Opisać oferowane parametry*
Interfejsy:		
Minimum 1 port 2,5GbE	DT	*Opisać oferowane parametry*
Minimum 1 port 1GbE	DT	*Opisać oferowane parametry*
Minimum 2 porty USB	DT	*Opisać oferowane parametry*
Transfer danych:		
Wydajność przesyłania danych minimum 290 Mb/s		*Opisać oferowane parametry*
Pamięć masowa:		
Minimum 2 dyski SATA o pojemności minimum 4 TB z możliwością wymiany		*Opisać oferowane parametry*
Wydajność zapisu/odczytu dysków, minimum 500 Mb/s		*Opisać oferowane parametry*
Wbudowana pamięć minimum 4 Gb	DT	*Opisać oferowane parametry*
Zarządzanie:		
Możliwość zarządzania z przeglądarki internetowej minimum Edge, Chrome		*Opisać oferowane parametry*
Możliwość konfiguracji urządzenia w trybie tworzenia kopii zapasowych, archiwizacji, dystrybucji oraz udostępniania danych.		*Opisać oferowane parametry*

Możliwość szyfrowania danych		*Opisać oferowane parametry*
Ochrona ransomware przy użyciu migawek		*Opisać oferowane parametry*
Certyfikaty i Deklaracje:		
Deklaracja zgodności UE (certyfikat CE) potwierdzająca spełnienie wymagań dyrektywy „Nowego Podejścia". Urządzenie musi posiadać oznakowanie CE.		*Opisać oferowane parametry*
Certyfikat zgodności z dyrektywą RoHS lub dokument wystawiony przez niezależną, akredytowaną jednostkę potwierdzający spełnienie kryteriów środowiskowych zgodnych z dyrektywą RoHS o eliminacji substancji niebezpiecznych		*Opisać oferowane parametry*
Deklaracja zgodności z dyrektywą WEEE lub oświadczenie producenta o spełnieniu obowiązków w zakresie postępowania z odpadami WEEE i zgodności z Ustawą z 11 września 2015 o zużytym sprzęcie elektrycznym i elektronicznym (Dz.U. 2015 poz.1688). Urządzenie musi być oznaczone etykietą WEEE.		*Opisać oferowane parametry*
INSTALACJA I MONTAŻ - odnosi się do całości zamówienia		
Zamawiający wymaga dostarczenia wszelkich komponentów potrzebnych do zamontowania dostarczonych urządzeń oraz do połączenia urządzeń do infrastruktury pasywnej (np. szyny montażowe, moduły światłowodowe, przewody krosowe, przewody zasilające, osprzęt montażowy).		
Wymagana instalacja dostarczonych urządzeń posiadających obudowę przeznaczoną do montażu stelażowego, we wskazanej przez Zamawiającego szafie RACK 19"za pośrednictwem szyn montażowych.		
Zamawiający wymaga wykonanie wszystkich połączeń urządzeń, niezbędnych do uruchomienia całości środowiska.		
Zamawiający wymaga instalacji wszystkich dostarczonych systemów na urządzeniach wskazanych przez Zamawiającego na etapie realizacji.		
KONFIGURACJA - odnosi się do całości zamówienia		
Przygotowanie środowiska udostępnionego przez Zamawiającego oraz jeżeli wymagane, infrastruktury informatycznej dostarczonej przez wykonawcę w celu możliwości uruchomienia rozwiązań.		
Na dostarczonych serwerach Wykonawca skonfiguruje środowisko wirtualne w oparciu o dostarczone systemy, a następnie zainstaluje serwery celem uruchomienia domeny i usług katalogowych zgodnie z wytycznymi Zamawiającego dostarczonymi na etapie realizacji.		

Należy wykonać migrację istniejących systemów i danych do środowiska zwirtualizowanego. Środowisko do zmigrowania:
- serwer Windows W2K3C aplikacyjno-usługowy,
- serwer Windows LBK bazodanowy i plików,
- serwer Linux PostgreSQL bazodanowy,
- serwer Linux bazodanowy wraz z bazami.

Rozbudowa systemu ochrony urządzeń o funkcjonalność XDR

Wykonawca zainstaluje na dostarczonym serwerze i skonfiguruje motor baz danych SQL w sposób zapewniający stabilną pracę modułu XDR. Jeżeli instalacja motoru baz danych będzie wymagała instalacji dodatkowych bibliotek programowych, należy je doinstalować.

W zakresie XDR należy skonfigurować i zoptymalizować reguły reagowania na incydenty oraz przygotować polityki połączeniowej i zaaplikowanie dla stacji końcowych z zainstalowanym konektorem.

W zakresie MFA uruchomić możliwość uwierzytelniania dwuskładnikowego przez użytkowników minimum z wykorzystaniem aplikacji mobilnej lub SMS.

W przypadku rozwiązania równoważnego:

a) przygotować pakiety instalacyjne i zainstalować system na wszystkich stacjach komputerowych;
b) przygotować wymagane polityki dla organizacji i działu IT;
c) skonfigurować polityki szyfrowania;
d) uruchomić wszystkie moduły;
e) włączenie domyślnych reguł zgodnie z wytycznymi Zamawiającego określonymi na etapie realizacji;
f) wykonać dokumentację zawierającą opis wszystkich modułów, punktów konfiguracji(wraz z rzutami ekranowymi, adresacjami, loginami wraz z hasłami, zalecenia wdrożeniowe;
g) przeprowadzić minimum 16 godzin instruktarzu stanowiskowego dla administratorów Zamawiającego zapewniającego pełne zrozumienie administracyjnych, instalacji oprogramowania systemowego i narzędziowego, znajomości i umiejętności realizacji procedur, znajomości wytycznych polityk bezpieczeństwa, potwierdzonego protokołem z wykonania instruktarzu.

Oprogramowanie DLP:

Instalacja i konfiguracja rozwiązania w środowisku Zamawiającego. Instalacja musi obejmować wszystkie stacje komputerowe.

W ramach konfiguracji Zamawiający wymaga:

a) włączenie funkcji audytora,
b) ustawienie tagowania minimum jednej przykładowej ścieżki lokalnej w oparciu o minimum 10 plików tekstowych,
c) ustawienie kategorii danych w oparciu o wskazane przez klienta dane wrażliwe,
d) ustawienie reguł DLP

DOKUMENTACJA POWYKONAWCZA
Po zakończeniu realizacji, Zamawiający wymaga dostarczenia pełnej dokumentacji powykonawczej oraz procedur eksploatacji rozwiązań. Dokumentacja powykonawcza musi zawierać minimum: a) opis ogólnych informacji o rozwiązaniach; b) schematy połączeń urządzeń i ich adresacje; c) zestawienie loginów i haseł do rozwiązań; d) zestawienie ustawień wszystkich rozwiązań; e) instrukcje instalacji, konfiguracji, uruchomienia; f) zestawienie licencji; g) listę autoryzowanych kontaktów serwisowych;
KRYTERIA RÓWNOWAŻNOŚCI
Serwerowy system operacyjny
Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości.
Wbudowane wsparcie instalacji i pracy na wolumenach które: - pozwalają na zmianę rozmiaru w czasie pracy systemu, - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, - umożliwiają kompresję „w locie” dla wybranych plików i/lub folderów, umożliwiają zdefiniowanie list kontroli dostępu (ACL).
Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
Uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

Wbudowana zapora internetowa (firewall) z obsługi definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
Graficzny interfejs użytkownika.
Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
Możliwość zmiany języka interfejsu po zainstalowaniu systemu dla co najmniej języka polskiego i angielskiego.
Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarzadzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: – podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, – ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
Zdalna dystrybucja oprogramowania na stacje robocze.
Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: a) dystrybucję certyfikatów poprzez http, b) konsolidację CA dla wielu lasów domeny, automatyczne rejestrowania certyfikat6w pomiędzy różnymi lasami domen.
Szyfrowanie plików i folderów.
Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
Serwis udostępniania stron WWW.
Wsparcie dla protokołu IP w wersji 6 (Ipv6).
Wbudowane usługi VPN pozwalające na zestawienie równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.