Załącznik Nr 1 do Zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Wykonawca może zaoferować tylko takie oprogramowanie, które w całości odpowiadają wymaganym minimalnym parametrom wskazanym przez Zamawiającego w poniższej tabeli.

Ilość licencji	2 - (dwie instalacje): 1. – 40 agentów 2. – 60 agentów
Architektura systemu	1. Agent – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej. 2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych). 3. Panel pracownika – aplikacja webowa dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej. 4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z agentami. 5. Baza danych pracująca na posiadanych przez urząd serwerach z systemem Windows Serwer 2012/2012R2/2016/2019/2022 6. Komponenty Agent, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu. 7. System musi umożliwiać komunikację pomiędzy agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem. 8. Wbudowany mechanizm automatycznej konserwacji/utrzymania zgodnie ze

	zdefiniowanym harmonogramem realizujący co najmniej: usuwanie zbędnych danych z systemu.
Wymagania systemowe	1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, Firefox, Chrome, Opera). 2. Agent musi pracować na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa. 3. Serwer www i bazy danych muszą działać na systemach 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 10/11. 4. Możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare. 5. Możliwość wielokrotnego, zgodnego z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej z usługi MS Active Directory.
Funkcjonalności systemu zarządzania infrastrukturą IT	1. Inwentaryzacja sprzętu komputerowego 1.1 umożliwia automatyczną inwentaryzację komputerów z zainstalowanym agentem znajdujących się w sieci lokalnej oraz poza siecią lokalną (za NATem) 1.2 zbiera szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation) oraz odczytuje informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania, a także skanuje dyski twarde (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART) 1.3 monitoruje parametry obciążenia komputerów: procesor, dyski, pamięć i sieć

	1.4 ewidencjonuje pliki na komputerach (nazwa, rozmiar, rodzaj, lokalizacja, w przypadku plików wykonywalnych: wersja, producent) oraz o zmiany w systemie plików (dodano plik, usunięto plik) 1.5 pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów. 1.6 umożliwia ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części). 1.7 umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja). 2. Inwentaryzacja urządzeń podłączanych do komputera 2.1 automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.) 2.2 pozwala na przypisanie podłączonego urządzenia do komputera oraz użytkownika. 2.3 umożliwia uzyskanie informacji kto, kiedy i na jakim komputerze posługiwał się urządzeniem zewnętrznym, pozwalając na jego jednoznaczne zidentyfikowanie. 2.4 umożliwia utworzenie dowolnej ilości list urządzeń USB dozwolonych do stosowania - tzw. białe listy urządzeń USB na podstawie zdefiniowanych reguł (dozwolone/niedozwolone) wg kryteriów: użytkownik, dzień tygodnia, okres (data od, godzina od, data do, godzina do), urządzenie USB, komputer, data obowiązywania reguły. 3. Inwentaryzacja urządzeń innych niż komputery 3.1. umożliwia inwentaryzację manualną dowolnych zasobów np. drukarki, switche, routery, monitory, pamięci masowe itp. 3.2. posiada wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym IP/porcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać SNMP w wersji 1/2c/3.

	3.3. skaner SNMP łączy zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port. 3.4. zbiera informacje o jakości połączenia: - czas odpowiedzi serwisów (usług) podawany w milisekundach: średni czas odpowiedzi, minimalny czas odpowiedzi, maksymalny czas odpowiedzi - ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat. 3.5 wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają agenta 3.6 system umożliwia niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci 3.7 system posiada bazę wzorców monitorowanych portów i usług. 3.8 posiada możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci, według dowolnych filtrów użytkownika. 3.9 umożliwia przypisanie urządzenia do użytkownika, ewidencję napraw, kosztów zakupu i serwisu, przypominania o upływającym terminie gwarancji oraz pozwala na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu. 3.10 pozwala na kopiowanie (duplikację) dowolnego urządzenia dowolną ilość razy. 4. Zarządzanie licencjami 4.1 szczegółowe informacje o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji) 4.2 ewidencja aplikacji i pakietów na komputerach oraz możliwość wykonywania audytów legalności, zdefiniowania listy aplikacji zabronionych a także zdalnego odinstalowania oprogramowania 4.3 odczyt identyfikatorów i kluczy produktowych dla systemu operacyjnego oraz dowolnego oprogramowania (tam gdzie jest

	technicznie możliwe). 4.4 wspiera następujące typy licencji: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value (Company wide), MOLP Open Value (non-Company wide), MOLP Open Value Subscription, CAL, SAAS, Trial, Shareware, Cal Per User. 4.5 umożliwia ewidencję licencji (data zakupu, cena, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT, nr zapotrzebowania) poprzez rejestrację dokumentów źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium. 4.6 zbiera informacje o uruchamianych aplikacjach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji, szczegóły aktywności użytkownika). 5. Zdalna administracja komputerami 5.1. wykonywanie poleceń powłoki, uruchamianie aplikacji, deinstalacja oprogramowania, zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika 5.2. skaner umożliwiający wykrywanie komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro, wersji Vpro, Serial Over LAN oraz zarządzanie komputerami z technologią Intel vPro, w tym: zdalne włączanie, wyłączanie komputera, konfiguracja BIOS, uruchomienie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji, połączenie się komputerem w trybie graficznym (od VPro v.6) 5.3. za pomocą technologii Ultra VNC: zdalne podłączenie do wielu komputerów jednocześnie, przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, poprawek i aktualizacji (service pack, patch). Umożliwia podłączenia do obecnie zalogowanego użytkownika oraz

	w trybie RDP (wylogowania użytkownika i przejęcia dostępu) 5.4. umożliwia zdefiniowanie dowolnego własnego zadania jednorazowego bądź cyklicznego z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, windows powershell. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status) 5.5. zezwala na wykonywanie zapytań WMI oraz edycję rejestrów bez zdalnego połączenia do urządzenia 5.6. umożliwia wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako) 5.7. ewidencja logowań użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie, tak w sieci lokalnej, jak i poza NAT 6. Zarządzanie magazynem IT 6.1. obsługa dowolnej ilości magazynów w różnych lokalizacjach 6.2. obsługa dokumentów PZ, WZ, MM+, MM-, LI 6.3. ewidencja materiałów w magazynach w oparciu o metodę FIFO (pierwsze przyszło pierwsze wyszło). 6.4. obsługa kodów kreskowych dla materiałów w magazynach 6.5. informacja o wartości materiałów w poszczególnych magazynach, aktualne stany magazynowe, dokumenty dotyczące danego materiału w dowolnym magazynie 6.6. możliwość przekazania zasobu z magazynu użytkownikowi lub urządzeniu. Dokument przekazania automatycznie zapisuje się na karcie szczegółowej osoby lub urządzenia, któremu zasób został przekazany oraz w dokumentach magazynowych 7. Repozytorium 7.1. możliwość dodawania nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów (znaczniki TAG) więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium w dowolnym miejscu systemu, uzyskanie informacji

	w jakich miejscach systemu dany dokument repozytorium występuje. 8. Kody kreskowe 8.1. generowanie kodów kreskowych (jedno i dwuwymiarowych) dla każdego zaewidencjonowanego urządzenia w standardzie wybranym przez użytkownika: aztec, codabar, code128, code39, dataMatrix, EAN128, EAN13, EAN8, interleaved2of5, ITF14, PDF417, POSTNET, qrcode, royalMailCBC, UPCA, UPCE, USPSIntelligentMail. 8.2. parametryzacja w zakresie wielkości graficznej kodu (wymiary, wielkość i typ czcionki) 8.3. możliwość zmiany typu i atrybutów kodu w dowolnym momencie, 8.4. informacja o błędzie generacji kodu, np. na skutek niewłaściwej długości wprowadzonego ciągu znaków w stosunku do danego standardu kodu. 8.5. możliwość masowego wydruku kodu / kodów. 8.6. obsługa kodów kreskowych nie może wymagać instalacji czcionek. 8.7. umożliwia współpracę z zewnętrznymi czytnikami kodów. 9. Komunikacja za pomocą wiadomości 9.1. tworzenie wiadomości tekstowych zgodne z HTML z możliwością eksportu / importu treści, celem automatycznego wysyłania do urządzeń, użytkowników lub dowolnych grup odbiorców, 9.2. wiadomości wysyłane jednorazowo lub cyklicznie zgodnie z definiowalnym harmonogramem 9.3. użytkownik otrzymujący wiadomość jest powiadamiany wizualne i dźwiękowo 9.4. wiadomości o podwyższonym priorytecie – alerty – wyświetlają się na środku ekranu, z widoczną treścią wiadomości 9.5. dla wiadomości innych niż alerty użytkownik ma możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania. 9.6. zabezpieczenie (np. synchronizowany z serwerem znacznik czasowy)

	odporne na zmiany czasu na lokalnym komputerze (użytkownika) a pozwalające na jednoznaczne ustalenie daty i godziny dostarczenia i odczytania wiadomości. 9.7. historia przesyłania wiadomości i odczytywania wiadomości przez użytkowników. 10. Monitorowanie drukarek sieciowych i wydruków 10.1. posiada możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa) 10.2. ewidencja wydruków obejmuje: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera z którego dokonano wydruku, format dokumentu, informację i jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor. 10.3. dla każdej z drukarek SNMP system musi udostępniać informacje: nr seryjny, IP, MAC, bieżący status drukarki, całkowitą ilość wydrukowanych stron, ilość wydrukowanych stron od uruchomienia, błędy, alerty, dostępne porty, stan pokryw, interfejsów sieciowych, rodzaj i ilości pamięci całkowitej i wykorzystanej, informacje o poziomie materiałów eksploatacyjnych 11. Monitorowanie stron www 11.1. posiada możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej. 11.2. ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek, również, gdy otwierana jest strona z połączeniem szyfrowanym (https) i obejmuje co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony, łączny czas korzystania, czas aktywności, czas pasywności 11.3. w oparciu o algorytmy sztucznej inteligencji system umożliwia analizę treści stron www oraz przypisanie im – w oparciu o treść – odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem odwiedzanych stron 11.4. każda odwiedzona strona powinna otrzymywać atrybuty: czy SSL, czy jest bezpieczna, czy zawiera przekierowania, czy znajduje się na

	liście CERT, czy znajduje się na liście stron hazardowych, czy kategoria strony jest bezpieczna, czy jest produktywna. 12. Monitorowanie dziennika zdarzeń 12.1. posiada możliwość monitorowania dziennika zdarzeń wszystkich komputerów 12.2. ewidencja zdarzeń następuje w oparciu o definiowalną kategorię zdarzenia: critical, error, warning, info, audit failure, audit success, debug oraz typ dziennika: aplikacja, bezpieczeństwo, system 12.3. pozwala na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia, musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia. 12.4. umożliwia monitorowanie komunikatów Syslog. 13. Repozytorium CMDB – centralna baza systemu umożliwiająca import i eksport danych zarówno poprzez API jak też za pomocą wbudowanego import/eksporta, na którą składają się: 13.1. Active Directory - lista serwerów LDAP, z których są importowane i aktualizowane dane o użytkownikach. System pozwala na wprowadzanie dowolnej ilości serwerów dla różnych domen. 13.2. kontenery dokumentów - grupy, do których można przypisywać zapisane w systemie dokumenty w celu sortowania. 13.3. kategorie aplikacji - lista kategorii, do których przynależą wykorzystywane przez użytkowników aplikacje. 13.4. komputery - lista zinwentaryzowanych komputerów, podzielonych wg typu autoryzacji. Widok rekordu zawiera szczegółowe dane dotyczące danego komputera. 13.5. dokumenty - repozytorium dokumentów zapisanych w systemie. 13.6. kategorie plików - lista typów plików kategoryzowanych przez system. Administrator ma możliwość zdefiniowania własnych grup, do których pliki będą przydzielane, według wpisanej maski. 13.7. pliki - lista zinwentaryzowanych plików ze wszystkich komputerów. 13.8. licencje - zestawienie licencji zapisanych w bazie systemu, które

	administrator może przypisywać do poszczególnych użytkowników. 13.9. typy licencji - lista typów licencji. 13.10. lokalizacje - lista zdefiniowanych lokalizacji, do których administrator może przypisać poszczególnych użytkowników. 13.11. typy urządzeń - lista typów urządzeń 13.12. urządzenia - lista urządzeń podzielonych wg typu. 13.13. producenci / Dostawcy - lista producentów i dostawców. 13.14. pamięć masowa - zestawienie dysków twardych z komputerów 13.15. porty sieciowe - lista monitorowanych portów sieciowych 13.16. usługi sieciowe - lista monitorowanych usług sieciowych 13.17. udostępnione zasoby sieciowe - lista udostępnionych zasobów sieciowych. 13.18. sieci - lista definiowalnych ręcznie sieci, do których administrator może ręcznie przypisywać komputery 13.19. systemy operacyjne - zestawienie unikalnych systemów operacyjnych 13.20. struktura org. - zestawienie struktur organizacyjnych zdefiniowanych bądź importowanych z Active Directory 13.21. kategorie procesów - lista kategorii, do których będą przypisywane procesy aplikacji uruchamianych przez użytkowników. Klasyfikacja procesów odbywa się za pomocą algorytmów sztucznej inteligencji 13.22. serwery - lista zinwentaryzowanych serwerów 13.23. usługi - zestawienie usług działających na komputerach 13.24. oprogramowanie - lista zinwentaryzowanego i monitorowanego oprogramowania 13.25. pamięć masowa USB - lista urządzeń pamięci masowej USB 13.26. administratorzy - lista administratorów i użytkowników systemu, z możliwością nadawania im indywidulanych uprawnień do wybranych funkcjonalności w systemie oraz danych użytkowników w ramach

	struktur organizacyjnych w zakresie przeglądania, edytowania, eksportowania i usuwania danych 13.27. użytkownicy / pracownicy - lista pracowników 13.28. kategorie WWW - lista kategorii stron WWW wykorzystywanych w procesie klasyfikacji stron internetowych. Klasyfikacja oparta o sztuczną inteligencję 13.29. serwisy WWW - lista monitorowanych serwisów WWW. 14. Eksport danych 14.1. możliwość wyeksportowania wybranych lub wszystkich danych do formatu xls, csv, pdf, OpenOffice calc, html, mht, xml, jpeg, png, gif, bmp. 14.2. posiada raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu), wieloinstancyjność raportowania (wiele otwartych raportów jednocześnie z wielu widoków) 14.3. generowanie raportu odbywa się po stronie serwera a nie klienta. 14.4. generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów 14.5. minimum 150 zdefiniowanych raportów dotyczących wszystkich obszarów funkcjonalnych 14.6. możliwość ustalenia harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu. 15. Powiadomienia 15.1. komunikaty w formie alertów w konsoli, wiadomości email wysyłanych na wybrane adresy oraz wiadomości SMS na wskazane numery telefonów 15.2. możliwość tworzenia wielu komunikatów w oparciu o te same zdarzenia z określeniem innych grup obiorców lub parametrów 15.3. możliwość edycji treści wysyłanych powiadomień oraz korzystania z danych umieszczonych w systemie w treści powiadomienia.

	15.4. System musi posiadać zdefiniowane powiadomienia dotyczące: używania zasobów zakazanych (pliki erotyczne i pornograficzne), braku skanowania komputerów, brakach w licencjach, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, wygasaniu serwisu lub licencji, upływającej gwarancji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu sieci, nadmiernym obciążeniu sieci na komputerze, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, wykryciu nowego oprogramowania lub jego odinstalowaniu, wykryciu niezgodność ze schematem oprogramowania, duplikatach adresów IP i MAC, dużej ilość danych wysyłanych przez dany port w switch'u, wykryciu nowych urządzeń w sieci, zmianie statusów portów w switch'u, podłączeniu niedozwolonego urządzenia USB, wykryciu zmiany w sprzęcie (WMI), błędach w dzienniku zdarzeń Windows, problemach z usługą systemu Windows 16. Automatyzacja 17.1 możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące wraz z częstotliwością wykonywania danej czynności (godzina, dzień, tydzień, miesiąc). 17.2zdefiniowane czynności wykonywane są automatycznie. 17.3dostępne mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów).
Monitorowanie i ochrona danych	1. Oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami. 2. System musi wspierać definiowanie nieograniczonej liczby znaczników (ang. fingerprint) i umożliwiać użycie ich do znakowania danych (plików). 3. System musi umożliwiać zdefiniowania bądź wykluczenia maski plików do oznakowania z wykorzystaniem znaków wieloznacznych,

	w konkretnych lokalizacjach lokalnych bądź sieciowych. 4. Znacznik nie może naruszać struktury pliku, w szczególności sygnatury podpisu cyfrowego, wielkości pliku i musi być niewidoczny dla użytkownika. 5. Jeden plik może być oznaczony dowolną ilością znaczników. 6. Zdejmowanie znaczników może być prowadzone w sposób manualny zdalnie przez administratora lub automatycznie, gdy reguła ustali, że znacznik powinien być zdjęty (np. plik w wyniku prowadzonej przez użytkownika edycji nie posiada już danych osobowych). 7. System musi automatycznie znakować pliki tworzone przez zdefiniowane procesy aplikacji, wybranych użytkowników. 8. System musi mieć możliwość automatycznego ustawiania / usuwania znaczników na plikach (np. txt, doc, docx, xls, xlsx, ppt, pptx) w oparciu o dowolnie zdefiniowaną zawartości (treści) pliku w postaci tekstu i wyrażenia regularnego. 9. System musi automatycznie wykrywać zdublowane pliki z wybranym znacznikiem.
Operacje w systemie plików	1. System musi monitorować zdarzenia otwarcia, usunięcia, utworzenia, zapisu, zmiany nazwy pliku w całym systemie plików. 2. System musi mieć możliwość zdefiniowania lokalizacji podlegających oraz wykluczonych z monitorowania oraz pozwalać na zdefiniowanie maski plików podlegających / wykluczonych z monitorowania z użyciem znaków wieloznacznych. 3. System musi mieć możliwość definiowania maski procesów, dla których dostęp do systemu plików będzie monitorowany. 4. System musi mieć możliwość stworzenia tzw. białej listy procesów, których dostęp do systemu plików nie będzie monitorowany. 5. System musi mieć możliwość monitorowania plików w oparciu o założone na pliki znaczniki.
Uruchamiane procesy i aplikacje	1. Podjęcie działania w momencie uruchomienia określonego procesu. 2. System musi mieć możliwość zdefiniowania dowolnej ilości reguł dotyczących uruchamiania procesu/aplikacji poprzez wykorzystanie maski zawierającej znaki wieloznaczne („*” oraz „?” zastępujące

	odpowiednio dowolny ciąg znaków oraz znak pojedynczy). 3. System musi mieć możliwość dołączenia bieżącego zrzutu ekranu do informacji o incydencie związanym z próbą uruchomienia monitorowanego procesu/aplikacji.