Samodzielny Publiczny Zakład Opieki Zdrowotnej
Wojewódzki Szpital Specjalistyczny nr 4 w Bytomiu
Aleja Legionów 10, 41-902 Bytom, NIP 626-25-10-567, REGON 000296271
tel. +48 323 964 500, e-mail: szpital@szpital4.bytom.pl, www.wss4.pl

Załącznik nr 2B do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. DZIAŁANIE

Projekt	382	Fundusz Przeciwdziałania COVID-19 działań w celu do podniesienia poziomu bezpieczeństwa systemów teleinformatycznych WSS4 w Bytomiu
Postępowanie	104	Zakup sprzętu komputerowego: sprzęt komputerowy dostawa i wdrożenie systemu DLP
Element	101	Opis przedmiotu zamówienia
Wersja	2	2022-11-18

2. OPIS

Dostawa i wdrożenie systemu DLP

Wykonawca dostarczy licencję minimum 3-letnią na użytkowane oprogramowania wraz z minimum rocznym wsparciem serwisowym i dostępnością aktualizacji.

Specyfikacja techniczna Systemu DLP (zabezpieczania danych przed wyciekiem)

Niniejszy dokument definiuje wymagania techniczne systemu DLP, zapewniającego kontrolę m.in. nad urządzeniami peryferyjnymi, w tym szczególnie urządzeniami podłączanymi poprzez porty USB oraz kontrolę poufnych danych wysyłanych poza sieć firmową, oferując równocześnie funkcjonalności szczegółowego raportowania rejestrowanych zdarzeń.

2.1 Parametry techniczno-funkcjonalne

1 System zapobiegania wyciekom danych i informacji (DLP).
2 Architektura / budowa
3 System musi umożliwić bezproblemową i stabilną obsługę co najmniej komputerów jednocześnie.
4 System musi posiadać architekturę:
5 Agent – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
6 Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Konsola musi pozwalać na realizację pełnego zarządzania systemem oraz komputerami, musi być wyposażona w mechanizmy do edycji/modyfikacji i analizy danych oraz zawierać wbudowany mechanizmy raportowania. Nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych czy też realizacji innych funkcji systemu.
7 Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z agentami.
8 Baza danych musi pracować na silniku Microsoft SQL Server.
9 Wszystkie komponenty systemu muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerem producenta systemu. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja agentów musi przebiegać w pełni automatycznie z wykorzystaniem wewnętrznej funkcjonalności systemu. W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie ze strony producenta paczki aktualizacyjnej w postaci jednego pliku z aktualizacją.
10 System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować niezbędne bazy wzorców, polityk, pomoc i inne wbudowane słowniki.
11 Agent do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI.
12 Agent musi być dostępny dla administratora z poziomu interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci sparametryzowanego wewnętrznie pliku msi (ustawione zmienne np. adres IP, port serwera) gotowego do zainstalowania
13 System musi zezwalać na wygenerowanie instalatora agenta, który umożliwi użytkownikowi instalację usługi bez posiadania poświadczeń administratora.
14 Agent musi być możliwy do zainstalowania za pośrednictwem MS Active Directory lub manualnie.
15 Agent musi pracować w trybie niewidocznym dla użytkownika (jako usługa systemowa).
16 System powinien umożliwiać generowanie unikatowego identyfikatora agenta (powtarzalnego dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, definiowalnego ciągu znaków lub losowego ciągu znaków.
17 Agent musi mieć definiowalny priorytet pracy (ABOVE_NORMAL, NORMAL, BELOW_NORMAL, IDLE).
18 Agent musi wspierać do sześciu różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i musi potrafić wykorzystać adres dostępny z puli adresowej w dowolnym momencie działania, bez konieczności restartu.
19 System musi umożliwiać komunikację pomiędzy agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.
20 System musi mieć możliwość współpracy komponentów agent i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami agentów.

21 System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem realizujące co najmniej: usuwanie zbędnych danych z systemu o definiowalnych parametrach retencji (w tym dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów), indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nieprzyrostowe, zmniejszanie bazy danych (tzw. shrink). Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie. System musi prezentować historię przeprowadzonych konserwacji/utrzymania.
22 Wymagania systemowe
23 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).
24 Agent musi działać na systemach 32 i 64 bitowych: Windows Server2012/2012R2/2016/2019/2022, 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.
25 Serwer musi działać na systemach 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11.
26 Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2012/2012R2/2016/2019/2022, Windows 10, Windows 11) oraz Java 8 (JRE lub JDK), Apache Tomcat 8+.
27 Baza danych musi działać na silniku Microsoft SQL Server 2012/2014/2016/2017/2019 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).
28 Jeśli architektura / wymagania systemu wymagają licencji typu CAL dla każdego komputera z zainstalowanym agentem należy dostarczyć wraz z systemem odpowiednią liczbę licencji CAL.
29 System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.
30 Interfejs
34 System musi umożliwiać wielokrotny (harmonogram), na życzenie, import użytkowników, struktury organizacyjnej z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej systemu.
35 Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.
36 System musi umożliwiać wsparcie dla SSL i TLS podczas importu z Active Directory.
37 System musi umożliwiać import użytkowników z dowolnego źródła danych, w tym z plików CSV, XLS, XLSX, MS SQL oraz baz danych MS SQL Server, MySQL, PostgreSQL poprzez definiowanie źródła danych, reguł importu (jakie pola/kolumny) oraz posiadać wbudowany harmonogram raportów.
38 System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS.
39 Funkcjonalności systemu
40 System musi monitorować i zapobiegać wyciekom danych (DLP) poprzez bieżące (w czasie rzeczywistym) monitorowanie działań użytkowników wg ściśle zdefiniowanych polityk bezpieczeństwa oraz reguł ich opisujących.
41 System musi prowadzić szczegółową bieżącą informację o zarządzanych komputerach.
42 System musi udostępniać podstawowe dane inwentaryzacyjne komputerów, m.in.: procesor, BIOS, pamięć, dyski twarde, tabela smart dysków, sieć, pliki, czas pracy, zdarzenia.
43 System musi zapewniać automatyczne uruchamianie ochrony zasobów w czasie rzeczywistym zgodnie ze zdefiniowanymi politykami.
44 System musi zapewniać ciągłą ochronę danych niezależnie od położenia komputera (w sieci lokalnej, sieci VPN, poza siecią).
45 System musi na bieżąco monitorować i chronić za pomocą odpowiednio zdefiniowanych polityk i reguł dane w ruchu, dane w spoczynku oraz dane w użyciu.
46 Przez dane w spoczynku rozumie się dane, które nie są (ale mogą być) w ruchu lub w użyciu, wymagają inwentaryzacji i zabezpieczenia.
47 Przez dane w użyciu należy rozumieć dane, które są aktywnie przetwarzane przez dowolną aplikację i/lub punkt końcowy (komputer). Przykłady danych w użyciu: edycja dokumentu MS Word, Excel, PowerPoint, edycja pliku tekstowego CSV, TXT, tworzenie pliku, przechwytywanie ekranu (screenshot), kopiowanie / wklejanie danych,
48 Wydruki.
49 Przez dane w ruchu należy rozumieć dane, które są przesyłane, np. kopiowanie danych (plików) z dysku sieciowego na nośnik USB, kopiowanie danych (plików) z komputera na komputer, przesyłanie danych e-mailem w treści lub w postaci załącznika, pobieranie danych z serwera FTP, przesyłanie danych za pomocą komunikatora.
50 System musi w pełni wspierać następujące polityki ochrony danych:
51 Zdefiniowanie schematu, w którym można określić, które aplikacje są zabronione, zalecane, dodatkowe bądź nieokreślone. Schemat oprogramowania można przypisać do dowolnej grupy komputerów. Mechanizm musi umożliwić automatyczne odinstalowanie oprogramowania, które wg zdefiniowanego schematu jest zabronione.
52 Oznaczanie na dowolnym komputerze (znakowanie przez agenta) określonych plików wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami.
53 Znakowanie określonych plików przechowywanych w zasobach serwerów lub udostępnionych zasobach (np. samodzielna macierz dyskowa) wybranymi, niewidocznymi, dowolnie zdefiniowanymi znacznikami, z wykorzystaniem harmonogramu.
54 Kontrolowanie wykonywania przez użytkowników operacji zrzutu ekranu.
55 Generowanie automatycznych zrzutów ekranu komputera w ramach ustalonego interwału czasowego wyrażonego w sekundach.
56 Umożliwienie powiadamianie o przekroczeniu dozwolonego czasu pracy komputera.
57 Podjęcie działania w momencie uruchomienia określonego procesu.
58 Monitorowanie określonych typów urządzeń przenośnych.
59 Monitorowania i blokowania operacji (otwieranie/ usuwanie/ tworzenie/ zapis/ zmiana nazwy) na plikach.
60 Zarządzanie dostępem do sieci społecznościowych, serwisów informacyjnych, blogów, bibliotek, forów dyskusyjnych oraz dowolnych stron www.
61 Wyświetlanie komunikatu na komputerach użytkowników podczas uruchamiania stacji roboczej. Komunikaty muszą być definiowalne z poziomu konsoli administracyjnej z wykorzystaniem edytora (możliwość utworzenia tabeli, dołączenia obrazu, wstawienia linku).
62 Monitorowanie danych przesyłanych za pomocą poczty e-mail oraz blokowanie przesyłania plików określonych typów.
63 Monitorowanie danych przesyłanych do chmury oraz blokowanie synchronizacji plików określonych typów z wybraną chmurą.
64 Blokowanie lub zezwalanie działania określonym typom urządzeń dostępnych w menedżerze urządzeń.

65 System musi pozwalać na zarzadzanie dostępem do telefonów komórkowych w trybie pamięci masowej, czytników kart pamięci i pendrive USB.
66 Podjęcie działań monitorowania i blokowania operacji w momencie próby kopiowania tekstu, zdjęcia czy ścieżki plików do schowka.
67 Blokowanie sieci ze względu na zdefiniowany typ i maskę sieci WIFI. Polityka musi zapewniać blokowanie dostępu do sieci zarówno otwartych jak i zabezpieczonych.
68 Regularne zdalne szkolenie (elearning) pracowników za pomocą definiowanej treści (html) z jednoczesnym prowadzeniem elektronicznej listy obecności. Wymagana jest możliwość zdefiniowania dowolnej ilości elementów (np. kompletów szkoleniowych z zakresu bezpieczeństwa) oraz wysyłanie ich do użytkowników zgodnie ze zdefiniowanym harmonogramem.
69 System musi być wyposażony w mechanizm tworzenia reguł ochrony (DLP) w oparciu o zdefiniowane polityki, obiekty docelowe, nazwy użytkowników, datę ważności polityki.
70 Obiekty docelowe reguł muszą być definiowalne za pomocą parametrów takich jak: nazwa komputera, adres IP, unikatowy identyfikator agenta, status podłączenia do systemu (online/offline), zainstalowany system operacyjny, nazwę zalogowanego użytkownika, model komputera, producent komputera, dostawca komputera, budżet, z którego zakupiony został komputer, strukturę organizacyjną
71 Przy definiowaniu obiektów docelowych dla reguł DLP można korzystać ze znaków wieloznacznych.
72 System musi posiadać funkcjonalności monitorowania, blokowania, powiadomieniu użytkownika o wystąpieniu naruszenia zdefiniowanej polityki oraz pełnego logowania zdarzeń dotyczących polityki dla celów administracyjnych (powiadomienie administratora systemu).
73 Monitorowanie i ochrona danych
74 System musi wspierać definiowanie nieograniczonej liczby znaczników (ang. fingerprint) i umożliwiać użycie ich do znakowania danych (plików).
75 System musi umożliwiać zdefiniowania bądź wykluczenia maski plików do oznakowania z wykorzystaniem znaków wieloznacznych, w konkretnych lokalizacjach lokalnych bądź sieciowych.
76 Znacznik nie może naruszać struktury pliku, w szczególności sygnatury podpisu cyfrowego, wielkości pliku i musi być niewidoczny dla użytkownika.
77 Jeden plik może być oznaczony dowolną ilością znaczników.
78 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).
79 System musi automatycznie znakować plików tworzone przez zdefiniowane procesy aplikacji, wybranych użytkowników.
80 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.
81 System musi automatycznie wykrywać zdublowane pliki z wybranym znacznikiem.
82 Zrzuty ekranu
83 System musi obsługiwać wielu ekranów (wiele monitorów podłączonych do jednego komputera).
84 System musi obsługiwać pulpity wirtualne (logiczny rozmiar pulpitu jest większy niż fizyczny rozmiar ekranu).
85 System musi mieć możliwość monitorowania/zablokowania wykonania zrzutu ekranu przez użytkownika za pomocą klawiatury.
86 System musi umożliwiać czytelny podgląd obrazów (zrzutów ekranowych) w konsoli administracyjnej.
87
88 Monitorowanie czasu pracy
89 System musi mieć możliwość zdefiniowania dowolnej ilości reguł dotyczących czasu pracy komputera.
90 System musi mieć możliwość zdefiniowania zalecanego czasu pracy dla każdego komputera, przy czym czas pracy w każdym dniu tygodnia może być zdefiniowany inaczej.
91 System musi mieć możliwość automatycznego dołączenia bieżącego zrzutu ekranu do każdego incydentu związanego z przekroczeniem zalecanego czasu pracy.
92 Uruchamiane procesy i aplikacje
93 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).
94 System musi mieć możliwość dołączenia bieżącego zrzutu ekranu do informacji o incydencie związanym z próbą uruchomienia monitorowanego procesu/ aplikacji.
95 Monitorowanie urządzeń przenośnych
96 System musi mieć możliwość utworzenia grup urządzeń przenośnych identyfikatora sprzętowego.
97 System musi automatycznie inwentaryzować (identyfikator sprzętowy, nazwa) podłączane do komputerów urządzenia przenośne.
98 System musi automatyczne rozpoznawać zaszyfrowane urządzenia przenośne z jednoczesnym odczytywaniem rodzaju klucza szyfrowania.
99 System musi mieć możliwość wykluczania grup urządzeń przenośnych z monitorowania (tzw. biała lista).
100 System musi mieć możliwość definiowania dni tygodnia oraz zakresu godzin, w których ma być aktywne monitorowanie urządzeń przenośnych.
101 System musi mieć możliwość jednoczesnego odczytania wielu identyfikatorów urządzeń przenośnych za pomocą multiplikatora portów USB poprzez wbudowaną do systemu funkcję lub aplikację.
102 System musi mieć możliwość dołączenia bieżącego zrzutu ekranu do każdego incydentu związanego z użyciem urządzenia przenośnego.
103 Operacje w systemie plików
104 System musi monitorować zdarzenia otwarcia, usunięcia, utworzenia, zapisu, zmiany nazwy pliku w całym systemie plików.
105 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.
106 System musi mieć możliwość definiowania maski procesów, dla których dostęp do systemu plików będzie monitorowany.
107 System musi mieć możliwość stworzenia tzw. białej listy procesów, których dostęp do systemu plików nie będzie monitorowany.
108 System musi mieć możliwość monitorowania plików w oparciu o założone na pliki znaczniki.
109 Dostęp do stron WWW
110 System musi mieć możliwość zdefiniowania maski stron podlegających monitorowaniu / blokowaniu za pomocą znaków wieloznacznych.
111 System musi mieć możliwość blokowania stron w oparciu o protokół nieszyfrowany (http) oraz szyfrowany (https).
112 System musi zapewnić wsparcie dla przeglądarek Opera w wersji nie niższej niż 63.0, Chrome w wersji nie niższej niż 77.0 oraz Firefox w wersji nie niższej niż 69.0.
113

114 Kanał poczty elektronicznej e-mail
115 System musi mieć możliwość zdefiniowania maski plików, które będą podlegały monitorowaniu/blokowaniu w zakresie ich użycia (wysyłania) w programach pocztowych za pomocą znaków wieloznacznych.
116 System musi wspierać rozwiązań poczty oparte o chmurę (np. Microsoft OWA).
117 Ochrona dostępu do rozwiązań opartych o chmurę
118 System musi mieć możliwość zdefiniowania masek plików, które będą podlegały monitorowaniu / blokowaniu w zakresie ich transmisji z lub do rozwiązania opartego o chmurę.
119 System musi wspierać co najmniej następujące rozwiązania oparte o chmurę: BitTorrent Sync, Box, Copy, Cubby, Dropbox, Google Drive, Knowhow Cloud, Mediafire, Mega, Microsoft OneDrive, Mozy, Spideroak, Strato HiDrive, Tresorit, Own Cloud.
120 Zabezpieczenia urządzeń
121 System musi mieć możliwość blokowania użycia grup urządzeń wg nazwy.
122 System musi mieć możliwość blokowania użycia grup urządzeń wg typu: stacje dysków CD-ROM/DVD, czujniki, czytniki kart inteligentnych, drukarki, GPS, imaging devices, karty graficzne, karty sieciowe, klawiatury, kontrolery dźwięku, wideo i gier, kontrolery IDE ATA/ATAPI, kontrolery IEEE 1394 Host Bus, kontrolery magazynu, kontrolery uniwersalnej magistrali szeregowej, kopie w tle woluminów magazynu, modemy, mysz i inne urządzenia wskazujące, napędy dyskietek, napędy taśmowe, PCMCIA adaptery, porty (COM i LPT), przenośne urządzenia z systemem Windows (WPD), software devices, stacje dysków, urządzenia akumulatorowe, urządzenia biometryczne, urządzenia Bluetooth, urządzenia interfejsu HID, urządzenia IrDA, urządzenia wielofunkcyjne, urządzenia zgodne ze standardem IEEE 1284.4, urządzenie USB, wieloportowe karty szeregowe, urządzenia Windows CE ActiveSync USB, woluminy magazynu, zmieniarki mediów.
123 System musi mieć możliwość dołączenia bieżącego zrzutu ekranu do informacji o incydencie związanym z zablokowaniem / odblokowaniem urządzenia.
124 Szyfrowanie dysków
125 System musi identyfikować partycje dysków twardych zaszyfrowane Bitlockerem.
126 System musi posiadać wbudowane mechanizmy do masowego zdalnego szyfrowania BitLockerem i wspierać metody XTS AES256, XTS AES128, AES256, AES128 oraz typy zabezpieczeń TPM+PIN, TPM, Passphrase.
127 Ochrona danych na budowanych dyskach twardych musi być realizowana przez silne szyfrowanie całej zawartości dysku/dysków oraz umożliwiać uwierzytelnianie użytkownika przed uruchomieniem startu systemu operacyjnego ze wsparciem metod silnego uwierzytelnienia.
128 Ochrona danych poprzez szyfrowanie całej zawartości dysku oznacza, że szyfrowaniu podlegają wszystkie informacje zapisane na dysku twardym (łącznie z systemem operacyjnym, sterownikami, zainstalowanymi programami, danymi itp.).
129 Funkcjonalność szyfrowania / deszyfrowania nie może być realizowana w oparciu o dodatkowego agenta na stacji roboczej, musi być integralnym rozwiązaniem oferowanego systemu.
130 System musi umożliwiać zdalne szyfrowanie / deszyfrowanie partycji systemowych oraz prezentować bieżący postęp tego procesu.
131 Proces szyfrowania odbywa się w sposób przezroczysty dla użytkownika komputera i może być realizowany w czasie jego pracy na komputerze. Szyfrowanie nie może być wyłączone przez użytkownika.
132 Proces szyfrowania może być zatrzymany podczas hibernacji oraz wyłączenia systemu ale jest kontynuowany po wzbudzeniu komputera / włączeniu.
133 System musi umożliwiać szyfrowanie / deszyfrowanie komputerów w sieci lokalnej oraz poza NATem.
134 Szyfrowanie urządzeń USB
135 System musi identyfikować partycje urządzeń USB zaszyfrowane Bitlockerem.
136 System musi posiadać wbudowane mechanizmy do masowego zdalnego szyfrowania BitLockerem i wspierać metody XTS AES256, XTS AES128, AES256, AES128 oraz typy zabezpieczeń TPM+PIN, TPM, Passphrase.
137 Ochrona danych na urządzeniach USB musi być realizowana przez silne szyfrowanie całej zawartości urządzenia.
138 Funkcjonalność szyfrowania / deszyfrowania nie może być realizowana w oparciu o dodatkowego agenta na stacji roboczej, musi być integralnym rozwiązaniem oferowanego systemu.
139 System musi umożliwiać zdalne szyfrowanie / deszyfrowanie urządzeń USB oraz prezentować bieżący postęp tego procesu.
140 Proces szyfrowania odbywa się w sposób przezroczysty dla użytkownika komputera i może być realizowany w czasie jego pracy na komputerze. Szyfrowanie nie może być wyłączone przez użytkownika.
141 Proces szyfrowania może być zatrzymany podczas hibernacji oraz wyłączenia systemu ale jest kontynuowany po wzbudzeniu komputera / włączeniu.
142 System musi umożliwiać szyfrowanie / deszyfrowanie urządzeń USB w sieci lokalnej oraz poza NATem
143 System musi umożliwiać zarządzanie dostępem do urządzeń usb poprzez definiowanie reguł blokujących dostęp do niezaszyfrowanych urządzeń.
144
145 Powiadomienia użytkowników
146 System musi mieć możliwość definiowania treści powiadomienia użytkownika komputera o naruszeniu przez niego polityki lub incydencie, zarówno z aktywnym blokowaniem incydentu (blokada i powiadomienie) jak i bez blokowania (tylko powiadomienie).
147 System musi mieć możliwość wykorzystania w komunikatach zmiennych systemowych (np. %UserName%, %FileName%, itp.), które w komunikacie dla użytkownika zostają automatyczne zastąpione rzeczywistymi danymi.
148 Powiadomienia administratorów
149 System musi prezentować wszystkie incydenty w konsoli administracyjnej oraz powiadamiać administratora o wystąpieniu incydentu za pomocą poczty e-mail w chwili jego wystąpienia.
150 Treść powiadomienia musi być definiowalna odrębnie dla każdej polityki DLP i musi umożliwiać wykorzystanie zmiennych systemowych (np. %UserName %, %FileName%, itp.), które w wysyłanym komunikacie zostają automatyczne zastąpione rzeczywistymi danymi.
151 System musi obsługiwać szyfrowane protokoły poczty e-mail.
152 System musi umożliwiać zdefiniowania dowolnej liczby odbiorców powiadomień.
153 Edukacja pracowników
154 System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów.
155 Formatowanie treści musi być zgodne z HTML.
156 System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych).
157 System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców.
158 Użytkownik otrzymujący wiadomość musi być powiadamiany wizualne i dźwiękowo o otrzymaniu nowej wiadomości.

159 Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.
160 System musi posiadać 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.
161 System musi udostępniać historię przesyłania i odczytywania wiadomości przez użytkowników.
162 System musi generować elektroniczną listę uczestników przeszkolonych.
163 Zdalne zarządzanie komputerami
164 System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, windows powershell.
165 Posiada bazę co najmniej 70 predefiniowanych poleceń.
166 System musi umożliwiać wywołanie zdefiniowanego zadania w chwili wystąpienia incydentu DLP.
167 System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, blokadę klawiatury i myszki, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji (service pack, patch).
168 System umożliwia zdalne podłączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC.
169 System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie.
170 Zarządzanie politykami bezpieczeństwa
171 System musi mieć możliwość konfiguracji i instalacji dowolnej ilości reguł dla dowolnych polityk DLP.
172 Instalacja polityk i reguł musi być możliwa do wykonania dla komputerów za NAT (bez VPN).
173 System musi mieć możliwość czasowej dezaktywacji danej reguły bez jej usuwania i utraty konfiguracji.
174 System musi mieć możliwość definiowania obiektów, na których działać będzie reguła w oparciu o parametry: nazwę komputera, adres IP, unikatowy identyfikator agenta, nazwę systemu operacyjnego, zalogowanego użytkownika, model komputera, strukturę organizacyjną, producenta komputera, dostawcę komputera, budżet z jakiego komputer został zakupiony.
175 Nowy komputer zgłaszający się do systemu po raz pierwszy musi bez dodatkowej ingerencji administratora automatycznie pobrać oraz wdrożyć (uruchomić) przeznaczoną dla niego politykę.
176 System musi mieć możliwość określenia ram czasowych działania danej reguły.
177 System musi dysponować mechanizmami dostępu do plików na poziomie jądra systemu operacyjnego MS Windows (32-bit i 64-bit), co uniemożliwia obejście zabezpieczeń nawet osobie z uprawnieniami administratora na poziomie systemu operacyjnego.
178 Raportowanie i eksport danych
179 System musi umożliwiać wyeksportowanie wybranych lub wszystkich danych do formatu .xls, .xlsx, .csv, .calc (OpenOffice), .html, .mht, .xml, .jpeg, .png, .gif, .bmp.
180 System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów, przy czym generowanie raportu musi odbywać się po stronie serwera www.
181 System powinien umożliwiać eksport danych z raportu do formatów: pdf, xls, doc, rtf.
182 System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).
183 System musi istnieć możliwość tworzenia i dodawania własnych raportów przez użytkownika.
184 Bezpieczeństwo
185 System musi umożliwiać definiowanie praw dostępu dla każdego użytkownika i grup użytkowników.
186 Kontrola dostępu musi być konfigurowana osobno dla każdego rodzaju operacji z puli: odczyt, zmiana, usunięcie, eksport.
187 System musi umożliwiać kontrolę dostępu jednocześnie na następujących poziomie menu aplikacji, wybranych typów poleceń (dodawanie, edycja, usuwanie, przeglądanie) i struktury organizacyjnej (np. administrator A ma dostęp tylko do informacji o urządzeniach przypisanych do struktury organizacyjnej S).
188 Uwierzytelnianie do systemu musi być realizowane:
189 Z wykorzystaniem imiennego konta użytkownika i hasła;
190 Z wykorzystaniem imiennego konta administratora i hasła;
191 Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej;
192 Za pośrednictwem jednokrotnego uwierzytelniania poprzez Active Directory;
193 Za pośrednictwem jednokrotnego uwierzytelniania poprzez CAS.
194 System musi udostępniać historię korzystania z poszczególnych opcji przez administratorów.
195 Siła hasła użytkownika musi być definiowalna w systemie w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków).
196 Przechowywanie haseł administratorów w bazie danych musi być poddane odpowiednio wysokiemu zabezpieczeniu. Hasła muszą być zapisywane jako base64 z (sól + SHA512 z login + hasło).
197 System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy agentami oraz serwerem, przy czym synchronizacja czasu nie wpływa na czas systemowy komputera z agentem.
198 System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz udostępniać informację o rezultacie wykonania kopii.
199 System musi zapewniać pełne logowanie błędów, przechowywanie logów systemowych, logów bezpieczeństwa, logów aktywności administratorów oraz posiadać możliwość eksportu logów.
200 System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.
201 Wsparcie i pomoc
202 System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim oraz dokumentację w postaci filmów instruktażowych w języku polskim.
203 Pomoc techniczna musi być świadczona w języku polskim w dni robocze w godzinach 8.00-16.00.

System musi wspierać następujące przykładowe zadania:
Spełnienie obowiązku szkoleniowego zgodnie z obowiązującymi wymogami np. rozporządzeniem RODO lub wewnętrzną polityką bezpieczeństwa. Działanie: Wykorzystanie gotowych, wbudowanych szkoleń z zakresu ochrony tajemnicy przedsiębiorstwa oraz możliwość tworzenia własnych treści szkoleniowych np. opartych o wewnętrzne regulaminy. W połączeniu z obowiązkiem potwierdzenia zapoznania się ze szkoleniem zapewnia wysoką skuteczność dystrybucji treści i podnoszenie świadomości pracowników w zakresie bezpieczeństwa IT.
Stworzenie klasyfikacji dla plików stanowiących dane istotne z punktu widzenia organizacji. Działanie: Możliwość łatwego i przejrzystego znakowania dokumentów pochodzących z wybranych aplikacji (np. aplikacji finansowo-księgowej) niewidocznymi znacznikami oraz oznaczanie dokumentów znajdujących się na serwerach plików zawierających np. umowy, porozumienia, dokumentacje projektowe.
Wprowadzenie zasad dostępu do plików. Działanie: Nadanie indywidualnych uprawnień określonym grupom pracowników do wybranych operacji na plikach np. umożliwienie grupie A jedynie odczytu, grupie B odczytu i modyfikacji, a grupie C zapewnienie nieograniczonego lecz monitorowanego dostępu, gdy jednocześnie grupa A, B, C posiadają nieograniczone uprawnienia nadane polityką Active Directory.
Nadzór i ograniczenie kanałów wycieku danych. Działanie: Wprowadzenie standardów przepływu plików w ramach aplikacji pocztowych, opartych o chmurę. Blokada możliwości przesyłania danych poprzez kanały komunikacyjne, takie jak: Bluetooth, IrDA, Wi-Fi.
Uświadamianie pracowników o naruszeniu przez nich polityki bezpieczeństwa. Działanie: Zdefiniowanie powiadomień nadrzędnych względem aktywnych okien użytkownika informujących o rodzaju naruszonej polityki.
Efektywne raportowanie stanu zabezpieczeń. Działanie: Dzięki dostępowi do konsoli zarządzającej poprzez dowolną przeglądarkę internetową (wspierającą HTML5) administrator z każdego urządzenia możne uzyskać swobodny dostęp do logów i raportów. Dzięki prowadzonej ewidencji można otrzymać statystyki osób generujących największą ilość incydentów bezpieczeństwa oraz mapę zagrożonych urządzeń i kanałów.
Uniemożliwienie wypływu poza organizację ważnych danych na nośnikach zewnętrznych. Działanie: Ograniczenie możliwości przenoszenia danych na nieautoryzowane nośniki zewnętrzne, takie jak: CD\DVD, pamięci masowe, urządzenia multimedialne.
Kontrola nad bezpieczeństwem przepływu danych w sieciach bezprzewodowych. Działanie: Uruchomienie polityki monitorującej podłączenia do sieci bezprzewodowych z możliwością zablokowania sieci otwartych, niezabezpieczonych, potencjalnie niebezpiecznych.

Administrator musi mieć możliwość nadania opisu dla konkretnej aplikacji, w celu łatwiejszej identyfikacji samej aplikacji jak i urządzenia na którym została ona zainstalowana.

---

3. INNE WYMAGANIA

1. Zakres prac

W ramach realizacji przedmiotu zamówienia Wykonawca:

- Dokona dostawy przedmiotu zamówienia, uruchomienie i konfigurację.
- Dokona instalacji i konfiguracji oprogramowania na serwerze
- Przeprowadzi instruktaże w zakresie użytkowania systemu dla personelu
- Przeprowadzi instruktaż w zakresie administrowania systemem
- Przekaże niezbędną dokumentacji powykonawczą
- Przekaże licencje bezterminowe, bez ograniczeń terytorialnych do oprogramowania

2. Dostawa

- Oferowane wyposażenie musi być fabrycznie nowe i nieużywane, pochodzić z bieżącej produkcji (rok produkcji – 2022),
- Koszty uruchomienia, konfiguracji, przekazania licencji oraz szkolenia personelu Zamawiającego ponosi Wykonawca. Dostawa nastąpi po wcześniejszym ustaleniu terminu, w dniu roboczym, w godzinach między 8:00 a 15:00.

3. Instruktaż

Wykonawca w ramach realizacji przedmiotu zamówienia przeprowadzi instruktaż pracowników Zamawiającego z zakresu prawidłowej obsługi dostarczonego systemu wraz z urządzeniami zgodnie z wymaganiami określonymi w SWZ.

4. Wsparcie techniczne

Usługa wsparcia technicznego przez okres min. 12 miesięcy dla zapewnienia ciągłości pracy oprogramowania poprzez wykonywanie w ramach usługi działań min.:

- Konsultacje telefoniczne dotyczące instalacji i eksploatacji oprogramowania opieka techniczna nad programem
- Świadczenie usług doradztwa technicznego obejmujące w szczególności.:
  - diagnozę oprogramowania w celu wykrycia sytuacji niepożądanych, w tym w szczególności monitorowanie zdarzeń zagrażających bądź potencjalnie zagrażających bezpieczeństwu systemu i właściwa reakcja na nie.
  - sprawdzenie poprawności działania aplikacji.
  - naprawa pojawiających się usterek.
- Przyjmowanie zgłoszeń Zamawiającego przy wykorzystaniu: infolinii (bezpośredni kontakt telefoniczny z konsultantem) oraz email (zgłaszanie problemów przez Internet)
- Czas reakcji serwisu technicznego od zgłoszenia awarii nie dłuższy niż 24 godziny od chwili zgłoszenia
- Czas usunięcia awarii nie dłuższy niż 5 dni roboczych.
- Przyjmowania zgłoszeń błędnego działania oprogramowania w godzinach 8:00 – 16:00 w dni robocze
- Świadczenie usług aktualizacji oprogramowania (o ile zostanie wydana przez Producenta).

5. Gwarancja

- Okres gwarancji liczony jest od daty podpisania protokołu odbioru bez zastrzeżeń.
- Gwarancja 24 miesiące.

6. Dokumentacja

Wykonawca wraz z dostawą przedmiotu umowy zobowiązany jest przekazać:

- Dokumentację dla użytkownika z obsługi oprogramowania w języku polskim
- Instrukcję wykonywania kopii bezpieczeństwa w języku polskim
- Instrukcja odzyskiwania danych z kopii bezpieczeństwa w języku polskim,
- Instrukcję dotycząca konfiguracji oprogramowania, w języku polskim
- Nośniki oprogramowania i dokumenty licencyjne producenta oprogramowania.