1 System antywirusowy z EDR, środowiskiem testowym i szyfrowaniem dysków na 250 stanowisk z licencją na 60 miesięcy.

1.1 Administracja zdalna

1.1.1 Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019, 2022 oraz systemach Linux.

1.1.2 Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.

1.1.3 Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.

1.1.4 Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.

1.1.5 Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.

1.1.6 Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.

1.1.7 Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

1.1.8 Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.

1.1.9 Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.

1.1.10 Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.

1.1.11 Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.

1.1.12 Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

1.1.13 Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym.

1.1.14 Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.

1.1.15 Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.

1.1.16 Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.

1.1.17 Serwer administracyjny musi posiadać wsparcie dla „VDI" oraz „Golden Master Image".

1.1.18 Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.

1.1.19 Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.

1.1.20 Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.

1.1.21 Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.

1.1.22 Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS.

1.1.23 Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP.

1.1.24 Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11.

1.1.25 Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap.

1.1.26 Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.

1.1.27 Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.

1.1.28 Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.

1.1.29 Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.

1.1.30 Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.
1.1.31 Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS.
1.1.32 Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
1.1.33 Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
1.1.34 Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
1.1.35 Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, 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 dla systemów Windows oraz MacOS z możliwością jego odinstalowania.
1.1.36 Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
1.1.37 Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.
1.1.38 W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.
1.1.39 Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
1.1.40 Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.
1.1.41 Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
1.1.42 Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.
1.1.43 Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
1.1.44 Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
1.1.45 Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
1.1.46 Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.
1.1.47 Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.
1.1.48 Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
1.1.49 Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
1.1.50 Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
1.1.51 Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.

1.1.52 Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
1.1.53 Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
1.1.54 Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
1.1.55 Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
1.1.56 Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.
1.1.57 Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
1.1.58 Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
1.1.59 Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.
1.1.60 Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
1.1.61 Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
1.1.62 Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta.
1.1.63 Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
1.1.64 Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
1.1.65 Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
1.1.66 Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.
1.1.67 Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
1.1.68 Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.
1.1.69 Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF lub CSV.
1.1.70 Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
1.1.71 Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
1.1.72 Powiadomienia mailowe mają być wysyłane w formacie HTML.
1.1.73 Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.
1.1.74 Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
1.1.75 Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
1.1.76 Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
1.1.77 Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.

1.1.78 Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
1.1.79 W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
1.1.80 Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
1.1.81 Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.
1.1.82 Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
1.1.83 Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
1.1.84 W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.
1.1.85 Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.
1.1.86 Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.
1.1.87 Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.
1.1.88 Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.
1.1.89 Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.
1.1.90 Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych.
1.1.91 Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault).
1.1.92 Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.
1.1.93 Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).
1.1.94 Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.

1.2 Szyfrowanie

1.2.1 System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10/11 32-bit i 64-bit.
1.2.2 System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
1.2.3 Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
1.2.4 Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.
1.2.5 Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.
1.2.6 Aplikacja musi mieć możliwość korzystania z technologii TCG OPAL - dyski sprzętowo szyfrowane.
1.2.7 Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
1.2.8 W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.
1.2.9 Aplikacja do szyfrowania musi być zarządzana z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej.

1.2.10 Konsola centralnego zarządzania musi pozwalać na wygenerowanie, dla każdej zaszyfrowanej stacji, dysku ratunkowego.
1.2.11 Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:
1.2.11.1 ilość znaków,
1.2.11.2 czy hasło ma zawierać wielkie litery,
1.2.11.3 czy hasło ma zawierać małe litery,
1.2.11.4 czy hasło ma zawierać cyfry,
1.2.11.5 czy hasło ma zawierać znaki specjalne,
1.2.11.6 okres ważności,
1.2.11.7 ilość nieudanych logowań,
1.2.11.8 możliwość zmiany hasła.
1.2.12 Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom.
1.2.13 Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku.

1.3 Sandbox w chmurze

1.3.1 Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
1.3.2 Rozwiązanie musi wykorzystywać do działania chmurę producenta.
1.3.3 Rozwiązanie musi posiadać 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.
1.3.4 Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
1.3.5 Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru
1.3.6 Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
1.3.7 Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
1.3.8 Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
1.3.9 Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
1.3.10 Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
1.3.11 Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
1.3.12 Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
1.3.12.1 Czysty,
1.3.12.2 Podejrzany,
1.3.12.3 Bardzo podejrzany,
1.3.12.4 Szkodliwy.
1.3.13 W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
1.3.14 W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.

1.4 EDR

1.4.1 Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych.
1.4.2 Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
1.4.3 System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.
1.4.4 Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
1.4.5 Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.

1.4.6 Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
1.4.7 Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
1.4.8 Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
1.4.9 Wykluczenia muszą dotyczyć procesu lub procesu „rodzica".
1.4.10 Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
1.4.11 Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
1.4.12 Serwer musi posiadać ponad 800 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
1.4.13 Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne.
1.4.14 Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
1.4.15 Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali.
1.4.16 Administrator musi posiadać 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.
1.4.17 Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
1.4.18 Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
1.4.19 W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
1.4.20 W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
1.4.21 Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy.
1.4.22 Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator 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.
1.4.23 Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal).
1.4.24 Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
1.4.25 Konsola administracyjna musi mieć możliwość tagowania obiektów.
1.4.26 Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli.
1.4.27 Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci.
1.4.28 Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
1.4.29 Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.

1.5 Agent

1.5.1 Pełne wsparcie dla systemu Windows 7/ 8/ 8.1/10/11 oraz Windows Server 2008/2012/2016/2019/2022.

1.5.2 Pełne wsparcie dla systemów macOS 10.12 i nowszych.

1.5.3 Wsparcie dla 32 i 64-bitowej wersji systemu Windows.

1.5.4 Agent musi współpracować z produktem antywirusowym tego samego producenta.

1.5.5 Agent nie może działać bez produktu antywirusowego tego samego producenta.

1.5.6 W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonanej przez agenta.

1.5.7 Połączenie agenta do serwera zarządzającego musi być szyfrowane.

1.5.8 Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane.

1.6 Dostawa, Gwarancja, licencje, wsparcie:

1.6.1 Termin dostawy – maksymalnie do 14 dni od dnia podpisania umowy.

1.6.2 Całość dostarczanego rozwiązania, tzn. każde z dostarczonych systemów, musi być objęte 60 miesięczną gwarancją.

1.6.3 Serwis gwarancyjny/licencyjny/wsparcie musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia przez cały okres obowiązywania gwarancji.

1.6.4 Zgłaszanie usterek/awarii poprzez pocztę elektroniczną, portal helpdesk lub infolinię.

1.6.5 Czas reakcji serwisu od momentu zgłoszenia - 1 godzina, czas na rozwiązanie zgłoszonej usterki/awarii - 24 godziny.

……

Data; kwalifikowany podpis elektroniczny
lub podpis zaufany lub podpis osobisty