



Fundusze Europejskie  
dla Świętokrzyskiego



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



WOJEWÓDZTWO  
ŚWIĘTOKRZYSKIE

## Załącznik nr 1 zapytania ofertowego nr 5/2024/BK

### Opis Przedmiotu zamówienia

#### OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup sprzętu elektronicznego i oprogramowania do zajęć w Liceum Ogólnokształcącym Mistrzostwa Sportowego w Ostrowcu Świętokrzyskim

w ramach projektu „Mistrzowski start w przyszłość”

Warunki uczestnictwa w postępowaniu:

1. Oferowany sprzęt ma być fabrycznie nowy, nieużywany oraz nieekspozowany na wystawach lub imprezach targowych, sprawny technicznie, bezpieczny, kompletny i gotowy do pracy, musi spełniać wymagania techniczno-funkcjonalne wyszczególnione w poniższym Opisie Przedmiotu Zamówienia.
2. W ramach przedmiotowego zamówienia, Zamawiający wymaga dostarczenia sprzętu i oprogramowania, którego parametry minimalne wskazane zostały poniżej. Zamawiający akceptuje sprzęt oraz oprogramowanie o wyższych (lepszych) parametrach użytkowych lub wykonany w nowszej technologii pod warunkiem, że produkty zaoferowane przez Wykonawcę spełniają wszystkie parametry minimalne.
3. Wykonawca w swej ofercie zawrze wszelkie koszty związane z dostarczeniem sprzętu.
4. Oferta Wykonawcy musi obejmować pełny określony zakres przedmiotu zamówienia.
5. Wszystkie oferowane produkty mają pochodzić z oficjalnego kanału dystrybucyjnego producenta, posiadać wszystkie wymagane certyfikaty i oznaczenia oraz spełniać wszystkie wymagane prawem normy.

## Zestawienie minimalnych parametrów technicznych na oferowany sprzęt oraz oprogramowanie

**I. Laptop – 16 sztuk**

Lp.	Nazwa funkcji/parametru	Wymagane minimalne parametry techniczne
	Przeznaczenie urządzenia	Cele edukacyjne, edycja tekstu, arkusze kalkulacyjne, prezentacje multimedialne, nauka zdalna. W ofercie wymagane jest podanie modelu, symbolu oraz nazwy producenta
1.	Procesor	- min. 13400 pkt wg PassMark Software na dzień 24.04.2024r.
2.	Dysk twardy	- min. 512 GB SSD M.2 NVMe
3.	Pamięć RAM	- min. 16 GB
4.	Ekran (matryca)	- matowy - rozdzielczość min. 1920x1080 (Full HD)
5.	Przekątna ekranu	- Nie mniejsza niż 15,6"
6.	Karta graficzna	- min. 2600 pkt wg PassMark Software na dzień 24.04.2024r.
7.	Dźwięk	- wbudowane głośniki 2szt - wbudowany min. jeden mikrofon
8.	Kamera	- minimum 720p
9.	Złącza	- USB 3.2, min. 2 szt. - USB Typu C, min. 1 szt. - HDMI – min. 1 szt. - RJ45 – min. 1 szt. - wyjście słuchawkowe / wejście mikrofonowe, min 1 szt.
10.	Bateria	- min. 3 komorowa
11.	Klawiatura	- QWERTY - wydzielona klawiatura numeryczna
12.	Oprogramowanie	Zainstalowany i zaktwowany oryginalny Microsoft Windows w wersji minimum 11 Home PL, system operacyjny umożliwi obsługę m.in.: plików wykonywalnych exe oraz plików skryptowych o rozszerzeniu ps1, cmd oraz bat. SID systemu Windows musi być unikalny dla każdego z dostarczonych laptopów a jego aktualizacje muszą być wykonane/zainstalowane po dniu podpisania umowy z Zamawiającym. W celu potwierdzenia legalności systemu wymagany jest min. sticker licencyjny.
13.	Gwarancja	min. 24 miesiące
14.	Informacje dodatkowe	Sprzęt musi być fabrycznie nowy, oryginalne pudełko producenta, sprzęt nie może być powystawowy

## II. Pakiet biurowy – 16 sztuk

L.p.	Nazwa parametru	Warunki równoważności dla oprogramowania biurowego wymagane przez Zamawiającego
1.	Dożywotnia licencja oprogramowania Microsoft Office w wersji 2021 Professional Plus dla edukacji lub równoważny, wymagany dokument potwierdzający prawo do korzystania z programu wraz z danymi zawierającymi informację umożliwiającą instalację	<p>Zamawiający uzna pakiet oprogramowania biurowego za równoważny, gdy spełni poniższe wymagania:</p> <ul style="list-style-type: none"> <li>- Praca w trybie off-line (brak konieczności podłączenia do Internetu) wraz z możliwością zapisania dokumentów na lokalnym dysku komputera.</li> <li>- Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych tylko o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu.</li> <li>- Oprogramowanie biurowe w najnowszej dostępnej na rynku wersji.</li> <li>- Dla oprogramowania musi być publicznie znany cykl życia przedstawiony przez producenta systemu i dotyczący rozwoju wsparcia technicznego – w szczególności w zakresie bezpieczeństwa. Wymagane jest prawo do instalacji aktualizacji i poprawek do danej wersji oprogramowania, udostępnianych bezpłatnie przez producenta na jego stronie internetowej w okresie co najmniej 5 lat.</li> <li>- Zamawiający wymaga, aby wszystkie elementy oprogramowania biurowego oraz jego licencja pochodziły od tego samego producenta.</li> <li>- Zawierające w pakiecie przynajmniej edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji, system obsługi relacyjnych baz danych, obsługę poczty e-mail.</li> <li>- Aplikacja do tworzenia prezentacji powinna umożliwiać udostępnianie prezentacji przy użyciu przeglądarki internetowej bez potrzeby instalowania dodatkowych elementów ani konfigurowania. Do każdej prezentacji można dodać wciągające wideo, aby zwrócić uwagę odbiorców. Nagrania wideo można wstawiać bezpośrednio w programie, a następnie dostosowywać je, przycinać lub oznaczać najważniejsze sceny w nagraniu zakładkami, aby zwrócić na nie szczególną uwagę. Wstawiane nagrania są domyślnie osadzone, dzięki czemu nie trzeba zarządzać dodatkowymi plikami wideo.</li> <li>- Pliki programów edytora tekstów, arkusza kalkulacyjnego i programu do tworzenia prezentacji można przechowywać online i uzyskiwać do nich dostęp, przeglądać, edytować i udostępniać innym użytkownikom.</li> </ul> <p>Pakiet biurowy musi spełniać następujące wymagania:</p> <ol style="list-style-type: none"> <li>1. Wymagania odnośnie interfejsu użytkownika: <ol style="list-style-type: none"> <li>a) Pełna polska wersja językowa interfejsu użytkownika;</li> <li>b) Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych;</li> <li>c) Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.</li> </ol> </li> </ol>

2. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki:
  - a) posiada kompletny i publicznie dostępny opis formatu;
  - b) ma zdefiniowany układ informacji w postaci XML;
  - c) umożliwia wykorzystanie schematów XML;
  - d) wspiera w swojej specyfikacji podpis elektroniczny.
3. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji oraz udostępniać narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców.
4. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropolecień, język skryptowy).
5. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
6. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
  - a) Edytor tekstów;
  - b) Arkusz kalkulacyjny;
  - c) Narzędzie do przygotowywania i prowadzenia prezentacji;
  - d) Narzędzie do zarządzania informacją prywatną (poczta elektroniczną, kalendarzem, kontaktami i zadaniami);
  - e) System obsługi relacyjnych baz danych.
7. Edytor tekstów musi umożliwiać:
  - a) Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty;
  - b) Wstawianie oraz formatowanie tabel;
  - c) Wstawianie oraz formatowanie obiektów graficznych;
  - d) Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne); e) Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków;
  - f) Automatyczne tworzenie spisów treści;
  - g) Formatowanie nagłówek i stopek stron;
  - h) Sprawdzanie pisowni w języku polskim;
  - i) Śledzenie zmian wprowadzonych przez użytkowników;
  - j) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności;
  - k) Określenie układu strony (pionowa/pozioma);
  - l) Wydruk dokumentów;
  - m) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną;

- n) Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, 2007, 2010, 2013, 2016 i 2019 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu;
- o) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji;

8. Arkusz kalkulacyjny musi umożliwiać:

- a) Tworzenie raportów tabelarycznych;
- b) Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych;
- c) Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu;
- d) Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice);
- e) Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych;
- f) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych;
- g) Wyszukiwanie i zamianę danych;
- h) Wykonywanie analiz danych przy użyciu formatowania warunkowego;
- i) Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie;
- j) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności;
- k) Formatowanie czasu, daty i wartości finansowych z polskim formatem;
- l) Zapis wielu arkuszy kalkulacyjnych w jednym pliku;
- m) Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, 2007, 2010, 2013 i 2019, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń;
- n) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

9. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

- a) Przygotowywanie prezentacji multimedialnych;
- b) Prezentowanie przy użyciu projektora multimedialnego;
- c) Drukowanie w formacie umożliwiającym robienie notatek
- d) Zapisanie jako prezentacja tylko do odczytu;
- e) Nagrywanie narracji i dołączanie jej do prezentacji;
- f) Opatrywanie slajdów notatkami dla prezentera;
- g) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo;
- h) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego;
- i) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w

	<p>źródłowym arkuszu kalkulacyjnym;</p> <p>j) Możliwość tworzenia animacji obiektów i całych slajdów;</p> <p>k) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera;</p> <p>l) Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, 2007, 2010, 2013, 2016 i 2019.</p> <p>10. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:</p> <p>a) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego;</p> <p>b) Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców;</p> <p>c) Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną;</p> <p>d) Automatyczne grupowanie poczty o tym samym tytule;</p> <p>e) Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy;</p> <p>f) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia;</p> <p>g) Zarządzanie kalendarzem;</p> <p>h) Udostępnianie kalendarza innym użytkownikom;</p> <p>i) Przeglądanie kalendarza innych użytkowników;</p> <p>j) Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach;</p> <p>k) Zarządzanie listą zadań;</p> <p>l) Zlecanie zadań innym użytkownikom;</p> <p>m) Zarządzanie listą kontaktów;</p> <p>n) Udostępnianie listy kontaktów innym użytkownikom;</p> <p>o) Przeglądanie listy kontaktów innych użytkowników;</p> <p>p) Możliwość przesyłania kontaktów innym użytkownikom</p> <p>11. System obsługi relacyjnych baz danych musi umożliwiać:</p> <p>a) tworzenie i przetwarzanie baz danych</p> <p>W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania</p>
--	---



## III. Program antywirusowy – 16 sztuk

L.p.	Nazwa parametru	Warunki równoważności dla oprogramowania biurowego wymagane przez Zamawiającego
1.	Program antywirusowy	<p>Zamawiający uzna program antywirusowy za równoważny, gdy spełni poniższe wymagania:</p> <ul style="list-style-type: none"> <li>- min. 2 letni</li> <li>- Administracja zdalna w chmurze <ul style="list-style-type: none"> <li>1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.</li> <li>2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.</li> <li>3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.</li> <li>4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.</li> <li>5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.</li> <li>6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.</li> <li>7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.</li> <li>8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.</li> <li>9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.</li> <li>10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.</li> <li>11. 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.</li> <li>12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.</li> </ul> </li> <li>- Ochrona stacji roboczych <ul style="list-style-type: none"> <li>1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).</li> <li>2. Rozwiązanie musi wspierać architekturę ARM64.</li> <li>3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</li> <li>4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.</li> <li>5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.</li> </ul> </li> </ul>



		<p>6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.</p> <p>7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.</p> <p>8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.</p> <p>9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.</p> <p>10. Rozwiązanie musi zapewniać 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).</p> <p>11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.</p> <p>12. Rozwiązanie musi posiadać 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.</p> <p>13. Rozwiązanie musi zapewniać 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, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.</p> <p>14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.</p> <p>15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:</p> <ul style="list-style-type: none"> <li>• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,</li> <li>• tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,</li> <li>• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,</li> <li>• tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,</li> <li>• tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.</li> </ul> <p>16. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z:</p>
--	--	--



		<p>zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.</p> <p>17. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.</p> <p>18. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>19. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antyvirus, antyspyware, metody heurystyczne).</p> <p>20. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p> <p>- Ochrona serwera</p> <p>1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.</p> <p>2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.</p> <p>3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.</p> <p>4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.</p> <p>5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.</p> <p>6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.</p> <p>7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.</p> <p>8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.</p> <p>Dodatkowe wymagania dla ochrony serwerów Windows:</p> <p>9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.</p> <p>10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).</p> <p>11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.</p> <p>12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.</p>
--	--	---

		<p>13. Rozwiązanie musi zapewniać administratorowi 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, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.</p> <p>14. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.</p> <p>15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.</p> <p>16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.</p> <p>17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.</p> <p>Dodatkowe wymagania dla ochrony serwerów Linux:</p> <p>18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.</p> <p>19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.</p> <p>20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.</p> <p>21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszzonego mikro-serwisu.</p> <p>- Ochrona urządzeń mobilnych opartych o system Android</p> <p>1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.</p> <p>2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.</p> <p>3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).</p> <p>4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.</p> <p>5. Rozwiązanie musi zapewniać wystanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:</p> <ol style="list-style-type: none"> <li>usunięcie zawartości urządzenia,</li> <li>przywrócenie urządzenie do ustawień fabrycznych,</li> <li>zablokowania urządzenia,</li> <li>uruchomienie sygnału dźwiękowego,</li> <li>lokalizację GPS.</li> </ol> <p>6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.</p> <p>7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:</p>
--	--	---



Fundusze Europejskie  
dla Świętokrzyskiego



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



WOJEWÓDZTWO  
ŚWIĘTOKRZYSKIE

		a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła.
--	--	--

### III. Urządzenie wielofunkcyjne – 1 sztuka

Lp .	Nazwa funkcji/parametru	Wymagane minimalne parametry techniczne
1.	Rozmiar papieru :	- A4
2.	Procesor:	- min. 1990 MHz
3.	Technologia wydruku:	- laserowa
4.	Druk w kolorze :	- tak
5.	Rozdzielczość kopiowania :	- min 600x600 dpi
6.	Pamięć RAM:	- min.512MB
7.	Predkość wydruku:	- min. 27 stron/min
8.	Języki drukowania:	- HP PCL 5e, HP PCL 6, emulacja HP postscript level 3, PWG Raster, PDF, URF, Native Office
9.	Porty :	- USB, Gigabit Ethernet
10	Typ skanera:	- płaski, automatyczny podajnik dokumentów
11	Wifi:	- tak

### IV. Monitor interaktywny – 1 sztuka

Lp .	Nazwa funkcji/parametru	Wymagane minimalne parametry techniczne
1.	Przekatna ekranu :	- min. 75"
2.	Rozdzielczość ekranu :	- min. 3840x2160 px
3.	Typ matrycy :	- IPS
4.	Jasność:	- min 390 cd/m2
5.	Kontrast statyczny :	- min 1200:1
6.	Uchwyt:	- tak
7.	Usługa montażu:	- tak