|  |
| --- |
| **Komputer przenośny specjalny** (lekki 14”) |
| **Parametr** | **Wymagane minimalne parametry techniczne** |
| Typ Urządzenia | Komputer mobilny będzie wykorzystywany dla potrzeb aplikacji biurowych, edukacyjnych, obliczeniowych, dostępu do Internetu oraz poczty elektronicznej. Nie dopuszcza się modyfikacji na drodze Producent-Zamawiający (np. modyfikacji lub wymiany jakiegokolwiek komponentu sprzętowego, wymagany system operacyjny musi być fabrycznie preinstalowany na etapie produkcji komputera. |
| Obudowa | Komputer charakteryzujący się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych. Oferowany model notebooka musi spełniać normy MIL-STD-810H w zakresie minimum:500.6 – niskie ciśnienie (wysokość) – procedura I, II501.7 – wysoka temperatura – procedura I, II502.7 – niska temperatura – procedura I,II503.7 – szok temperaturowy – procedura I-A,I-B505.7 – promieniowanie słoneczne (wystawienie na światło słoneczne) – procedura I, II507.6 – wilgotność - procedura II510.7 – piasek i kurz - procedura I, II511.7 – atmosfera łatwopalna – procedura I514.8 – wibracje – 514.8C-2, 514.8C-6, 514.8C-8, 5148E-1516.8 – szok (uderzenie) – procedura I,II,IV,V,VI524.1 – zamrażanie / odmrażanie – procedura III (nagła zmiana temperatury)528.1 – wibracje – procedura IJednoznaczne informacje na temat powyższej certyfikacji MIL-STD 810H muszą znajdować się w ogólnodostępnej dokumentacji technicznej producenta komputera. W powyższym zakresie nie dopuszcza się modyfikacji konstrukcji, re-certyfikacji itp. na drodze Producent – Zamawiający. |
| Ekran | * matryca TFT 14” z podświetleniem w technologii LED;
* proporcje matrycy 16:10
* rozdzielczość min. FHD 1920x1200
* odwzorowanie kolorów 100% sRGB
* technologia IPS;
* jasność min. 400nits;
* Kąt otwarcia pokrywy ekranu min.180 stopni
* Ekran matowy;
* Obudowa mechanizmu otwierania matrycy (zawiasów) w całości wykonana ze stopów metali celem pełnego zabezpieczenia wrażliwych elementów na uszkodzenia mechaniczne;
* Parametry potwierdzone w ogólnodostępnej dokumentacji producenta komputera;
 |
| Wymiary obudowy | Suma wymiarów obudowy mierzona w najszerszych jej miejscach (wysokość, szerokość, głębokość) nie przekracza 570mm, w tym grubość w najgrubszym miejscu obudowy bez uwzględnienia nóżek nie przekracza 18mm; |
| Waga | Waga typowa wraz z oferowanym akumulatorem według oficjalnej dokumentacji producenta komputera – max. 1,19kg; |
| BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera.BIOS musi oferować graficzne menu i wbudowaną obsługę wskaźnikiem (wbudowany touchpad)Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez uruchamiania jakiegokolwiek dodatkowego oprogramowania z zewnętrznych i podłączonych do komputera urządzeń odczytania bezpośrednio z BIOS (poprzez dostępny interfejs graficzny) informacji o:1. model i producent oferowanego komputer (pełna nazwa handlowa)
2. konfiguracja fabryczna (unikalny kod konfiguracji)
3. unikalny kod „asset tag” możliwy do zapisania narzędziami dostarczonymi przez producenta (nieedytowalny z BIOS)
4. wersji i data publikacji BIOS
5. unikalny nr seryjnym komputera
6. unikalny nr seryjny płyty głównej
7. model zainstalowanego procesora wraz z taktowaniem bazowym
8. Ilości zainstalowanej pamięci RAM
9. UUID;
10. ilość i typ rdzeni obliczeniowych procesora;

Musi istnieć bezpośrednia możliwość eksportu informacji zawartych w punktach a) – i) za pośrednictwem kodów QR (bezpośrednio z poziomu BIOS) celem łatwego katalogowania i identyfikacji komputera;* Informacja o licencji preinstalowanego systemu operacyjnego, która została zaimplementowana w BIOS (widoczna na poziomie BIOS)
* Wsparcie dla technologii Microsoft Device Guard;
* Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:
* Możliwość ustawienia hasła Administratora
* Możliwość ustawienia hasła Użytkownika
* Możliwość ustawienie osobnego hasła wymaganego do uruchomienia komputera niezwiązanego z hasłem Administratora
* Możliwość ustawienia hasła dysku twardego
* Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS
* Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej.
* Możliwość Wyłączania/Włączania: karty sieciowej, karty sieciowej Wifi, czytnika linii papilarnych, mikrofonu, głośników, zintegrowanej kamery, czytnika kart SD, portów USB, Bluetooth, osobno interfejsu Thunderbolt;
* Komputer musi obsługiwać dedykowane, fabryczne stacje dokujące (komunikacja poprzez interfejsy USB-C i Thunderbolt) -Obsługa WoL za pośrednictwem połączenia poprzez stację dokującą, obsługa MAC Address Pass Through;
* BIOS musi umożliwiać uruchomienie funkcji bezpieczeństwa pozwalającej na przywrócenie poprzedniej wersji BIOS w przypadku uszkodzenia lub działań nieporządanych (np. malware itp.)
* Możliwość konfiguracji trybu pracy komputera bezpośrednio w BIOS – co najmniej: maksymalna wydajność, tryb zbalansowany;
* Komputer musi posiadać wbudowaną technologię usuwania danych z wbudowanego dysku SSD na poziomie BIOS (bez użycia narzędzi i oprogramowania zewnętrznego);
 |
| Zintegrowany system diagnostyczny | * Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia błędów zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego.
* Działający w zakresie całej funkcjonalności nawet w przypadku uszkodzenia dysku twardego.
* System umożliwiający wykonanie minimum następujących czynności diagnostycznych (umożliwiający eksport raportu testów za pomocą kodów QR):
* wykonanie testu: pamięci RAM, procesora, pamięci masowej nVme, matrycy LCD, magistrali pci-e, płyty głównej (chipset, usb), karty audio i wbudowanych głośników, klawiatury i touchpad, baterii,
* identyfikację jednostki i jej komponentów w następującym zakresie: notebook (producent, numer konfiguracji, model, numer seryjny), bios (wersja oraz data wydania bios), procesor (nazwa, taktowanie maksymalne, ilości pamięci L1, L2, L3, liczba rdzeni oraz wątków), pamięć ram (ilość zainstalowanej pamięci ram, producent oraz numer seryjny poszczególnych kości pamięci wraz z obsadzeniem, taktowanie pamięci), dysk twardy (model, numer seryjny, wersja oprogramowania sprzętowego, pojemność, temperatura), LCD (producent, model, rozdzielczość), bateria (data produkcji i data pierwszego użycia, pojemnośc, temperatura, napięcie, stopień naładowania)
* dsd-odczyt informacji SMART dla wbudowanego dysku SSD nVME
 |
| Płyta główna | Płyta główna zaprojektowana i wyprodukowana przez producenta oferowanego komputera lub na jego zlecenie, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego modelu urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej. |
| Procesor | Procesor wielordzeniowy ze zintegrowaną kartą graficzną, zaprojektowany do pracy w komputerach przenośnych, osiągający w teście „PassMark - CPU Mark” wynik co najmniej 17 250 pkt (zgodnie z załącznikiem A1). |
| Pamięć operacyjna RAM | Min. 16 DDR5 |
| Wbudowana pamięć masowa | Wbudowany fabrycznie dysk M.2 min. 510 GB SSD PCIe NVMe Gen.4 |
| Karta graficzna | Zintegrowana z procesorem, osiągająca w teście „PassMark - G3D Mark” wynik co najmniej 2 660 pkt. (zgodnie z załącznikiem A2). |
| Multimedia | * Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition;
* Trwale wbudowane w obudowie komputera cztery głośniki (Sumaryczna moc min 5,5W), port słuchawek i mikrofonu typu COMBO
* Fabrycznie zintegrowana w obudowie matrycy kamera video FHD, hybrydowa z funkcją IR (obsługa Windows Hello) oraz z mechaniczną zasłoną obiektywu;
* wbudowane cztery mikrofony, zintegrowana technologia Dolby Voice;
* Sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute);
 |
| Zdalne Zarządzanie | Wbudowana w płytę główną technologia zarządzania i monitorowania komputerem na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4 oraz IPv6, a także zapewniająca:1. monitorowanie konfiguracji komputera na poziomie komponentowym (Rodzaj, model, pojemność): CPU, Pamięć, HDD wersja BIOS płyty głównej;
2. zdalną konfigurację ustawień BIOS (BIOS setup),
3. możliwość zdalnego zarządzania stanem zasilania komputera: włączenie/wyłączenie/reset/poprawne zamknięcie systemu operacyjnego,
4. zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego z wirtualnego nośnika FDD/ CD ROM/DVD/Boot USB lub pliku obrazu bootującego takiego nośnika z serwera zarządzającego
5. zdalne przejęcie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości minimum 2560x1600.
6. technologia zarządzania i monitorowania komputerem na poziomie sprzętowym powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (<http://www.dmtf.org/standards/wsman>) oraz DASH 1.0.0 (<http://www.dmtf.org/standards/mgmt/dash/>)
7. nawiązywanie przez sprzętowy mechanizm zarządzania, zdalnego szyfrowanego protokołem SSL/TLS połączenia z predefiniowanym serwerem zarządzającym, w definiowanych odstępach czasu, w przypadku wystąpienia predefiniowanego zdarzenia lub błędu systemowego (tzw. platform event) oraz na żądanie użytkownika z poziomu BIOS.
8. sprzętowy firewall zarządzany i konfigurowany wyłącznie z serwera zarządzania oraz niedostępny dla lokalnego systemu OS i lokalnych aplikacji
9. ww. wbudowana w płytę główną technologia zarządzania i monitorowania komputera na poziomie sprzętowym - powinna pozwalać na konfigurację parametrów funkcji zarządzania (m.in. parametrów kont uprawnionych do zarządzania sprzętowego) każdym z następujących mechanizmów:
* lokalnie (na komputerze zarządzanym), bez udziału systemu operacyjnego - tj. z poziomu modułu BIOS przy użyciu pliku parametrów konfiguracji na nośniku USB. Należy dostarczyć odpowiednie narzędzie/oprogramowanie do tworzenia pliku parametrów konfiguracji na nośnik USB.
* zdalnie poprzez sieć LAN z wykorzystaniem szyfrowanego połączenia – za pomocą narzędzia/oprogramowania konfigurującego z wykorzystaniem wbudowanego  w technologię mechanizmu weryfikacji predefinowaych certyfikatów cyfrowych /kluczy asymetrycznych. Należy dostarczyć lub wskazać odpowiednie bezpłatne narzędzie do definiowania pliku parametrów konfiguracji oraz narzędzie/oprogramowanie konfigurujące.
* lokalnie (na komputerze zarządzanym) z poziomu systemu operacyjnego przy użyciu odpowiedniego narzędzia. Należy dostarczyć lub wskazać odpowiednie bezpłatne narzędzie do definiowania pliku parametrów konfiguracji oraz narzędzie/oprogramowanie konfigurujące.
* wymagana jest obsługa  autentykacji dla  HTTP Digest/ HTTPS Digest  z obsługą co najmniej 8 użytkowników Digest  oraz  Kerberos  z obsługą co najmniej 16 użytkowników lub grup AD

Wymagana jest obsługa autentykacji (wbudowany suplikant) autentykacji 802.1x na poziomie technologii sprzętowego zarządzania – przed uruchomieniem/bez uruchomienia OS. |
| Zintegrowane w obudowie interfejsy komunikacyjne | * min. 2x Thunderbolt 4;
* minimum 2x USB-A 3.2, w tym minimum jeden port musi umożliwiać ciągłą funkcję ładowania (tzw. Always Power On lub podobne);
* wsparcie producenta komputera dla stacji dokujących Thunderbolt 4 / USB-C dostępnych w ofercie producenta oferowanego modelu komputera;
* min. 1 złącze słuchawek i złącze mikrofonu typu COMBO;
* min. 1 xHDMI 2.1,
 |
| Karta sieciowa WLAN, komunikacja bezprzewodowa; | * Wbudowana karta sieciowa WLAN, pracująca w standardzie min. AX;
* Bluetooth min. 5.2;
* Zintegrowane anteny komunikacji 4G oraz złącze kart nano-SIM (tacka karty SIM dostępna bez konieczności rozkręcania obudowy komputera);
 |
| Klawiatura i urządzenia wskazujące | * Klawiatura odporna na zalanie cieczą (potwierdzone w ogólnodostępnej dokumentacji producenta komputera), układ US;
* Klawiatura wyposażona w 2 stopniowe podświetlanie przycisków włączane kombinacją klawiszy bezpośrednio z klawiatury komputera;
* dedykowana diodowa sygnalizacja włączenia przycisku CapsLock;
* diodowa sygnalizacja włączenia przycisków funkcyjnych w linii klawiszy F1-F12;
* przycisk włączania komputera musi znajdować się poza obrysem klawiatury, celem uniknięcia przypadkowego naciśnięcia – nie dopuszcza się umiejscowienia przycisku włączania np. w górnym rzędzie klawiatury, w dowolnym miejscu;
* musi być możliwość natychmiastowego i niezależnego wyciszenia mikrofonów i głośników osobnymi dedykowanymi klawiszami funkcyjnymi – funkcje te muszą posiadać dedykowaną sygnalizację diodową niezależną dla każdej z nich;
* klawiatura musi posiadać dedykowane przyciski funkcyjne do odbierania i zakończania rozmowy telekonferencyjnej oraz osobny przycisk uruchamiający okno chat;
* wbudowany touchpad z 3 przyciskami (każdy jako niezależny fizyczny przycisk – nie dopuszcza się wspólnej obudowy z uwagi na łatwość użycia przez użytkowników niezaawansowanych);
 |
| Bezpieczeństwo | * Wbudowany czytnik linii papilarnych w przycisku zasilania (typu Match on chip)
* Zintegrowany TPM 2.0 (dedykowany układ sprzętowy bezpośrednio na płycie głównej, niezintegrowany z chipsetem płyty głównej)
* Slot typu Kensington
* Fabrycznie wbudowany czujnik otwarcia obudowy. Dostęp do podzespołów komputera musi być sygnalizowany przez czujnik otwarcia obudowy. Sygnalizacja konfigurowana z poziomu BIOS, możliwość zablokowania uruchomienia komputera w przypadku wykrycia zadziałania funkcji czujnika;
* Mechaniczna zasłona kamery wbudowana trwale w ekran komputera na etapie produkcji (nie dopuszcza się elementów instalowanych poprodukcyjnie, naklejanych itp.);
* Dysk systemowy zawierający funkcję recovery umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii;
 |
| Bateria | * Min.57Wh;
* Czas pracy wg testu MobileMark 2018 – min. 13h (potwierdzony w ogólnodostępnej dokumentacji producenta lub wymaga się dołączania testu dla oferowanego komputera)
* Dedykowana dioda pozwalająca na optyczną weryfikację stanu ładowania baterii komputera przy zamkniętej matrycy;
* System szybkiego ładowania baterii – minimum 80% w ciągu 60 minut;
* Komputer dostarczony z fabryczną ładowarką USB-C/ Thunderbolt min. 65W;
 |
| System Operacyjny, certyfikowane systemy | Preinstalowany system operacyjny Microsoft Windows 11 Pro 64 bit, dostarczona licencja Microsoft Windows 11 Pro; |
| Oprogramowanie zintegrowane  | Oprogramowanie producenta oferowanego sprzętu umożliwiające:* automatyczna weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika;
* Możliwość weryfikacji z poziomu systemu operacyjnego Windows: model komputera, numer seryjny komputera, wersja BIOS, statusu gwarancji (czas rozpoczęcia, czas zakończenia), status baterii (data produkcji, naładowanie, temperatura, ilość odbytych cykli ładowania, pojemność znamionowa w Wh, pojemność po pełnym naładowaniu w Wh, możliwość włączenia/wyłączenia szybkiego trybu ładowania akumulatora, możliwość włączenia/wyłączenia trybu przedłużenia żywotności akumulatora w przypadku pracy na zasilaczu, włączenie/wyłączenie funkcji ładowania urządzeń zewnętrznych poprzez port USB w przypadku gdy komputer jest wyłączony, w trybie hibernacji lub uśpienia)
* scentralizowane zarządzanie zabezpieczeniami w tym: ochroną antywirusową, zapora firewall, aktualizacjami Windows, czytnikiem linii papilarnych;
* wbudowana ochrona przed potencjalnie niebezpiecznymi sieciami Wifi;
* Wbudowana na poziomie systemu operacyjnego Windows aplikacja pozwalająca na scentralizowane testowanie sprzętu: CPU, pamięć RAM, sieć WIFI (siła sygnału, zasięg, anteny), wbudowany dysk twardy SSD);
 |
| Certyfikaty | Wymagania dla producenta sprzętu: * ISO 9001 (należy załączyć do oferty).
* ISO 14001
* ISO 50001

Komputer musi spełniać następujące normy:* EPEAT Gold
* ENERGY STAR 8.0
* TCO Certified 9.0
* Deklaracja zgodności CE (należy załączyć do oferty).
* Zgodność z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych
 |
| Oprogramowanie do wykonywania kopii zapasowej systemu operacyjnego | Jedna licencja lub subskrypcja z wsparciem na min. 12 miesięcy, spełniająca poniższe wymagania:* Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
* Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
* Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
* Rozwiązanie musi wspierać system operacyjny macOS
* Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
* Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
* Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
* Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
* Rozwiązanie musi wspierać backup podłączonych dysków USB
* Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
* Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
* Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
* Rozwiązanie musi wspierać kontrolę pasma sieciowego
* Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
* Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
* Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
* Rozwiązanie musi wspierać technologię BitLocker
* Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
* Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
* Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
* Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.
* Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
* Rozwiązanie musi wspierać szyfrowanie
* Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
* Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
* Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
* Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
 |
| Moduł rozszerzenia programu antywirusowego EDR (Endpoint Detection and Response) | Zamawiający posiada oprogramowanie antywirusowe firmy ESET. Wymagane jest dostarczenie licencji bezterminowej z wsparciem technicznym przez okres min. 12 miesięcy na moduł EDR dla oprogramowania firmy ESET lub licencję systemu EDR dowolnego producenta, spełniającą poniższe wymagania:* Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS pracujący równocześnie z systemem antywirusowym ESET do ochrony stacji roboczych
* Rozwiązanie musi zawierać centralną konsolę administracyjną umożliwiającą monitorowanie oraz wizualizację zebranych danych z zarządzanych urządzeń.
* Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej.
* Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
* Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia.
* Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, nazwę komputera, grupę, użytkownika.
* Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, rozmiar pliku.
* Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne lub niebezpieczne.
* Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.
* Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania komend zdalnych.
* Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
* Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
* Rozwiązanie musi umożliwiać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
* Rozwiązanie musi zapewniać integrację z przynajmniej takimi systemami jak: konsola programu antywirusowego, moduł EDR.
* Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: numer seryjny, informacje o systemie, procesor, pamięć RAM, karty sieciowe.
* Serwer administracyjny musi posiadać możliwość tworzenia grup komputerów.
* Rozwiązanie musi zapewniać korzystanie z min. 100 szablonów raportów, przygotowanych przez producenta lub własnych raportów tworzonych przez administratora.
* Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email oraz do dziennika syslog.
* Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami.
* Rozwiązanie musi informować administratora o niezainstalowanych aktualizacjach systemowych.
 |
| Dodatkowe wyposażenie | * Mysz bezprzewodowa 2,4Ghz, optyczna, rozdzielność pracy min. 900 dpi, min. 5 przycisków, wymiary max. 110 x 75 x 45 mm, waga max. 140 g
* Torba na notebook 14”, wymiary max. 39 x 9 x 35 cm, Polyester, rączka, pasek na ramię, kieszeń zewnętrzna na zamek
* Adapter USB-C do RJ45, min. Ethernet 100Base-TX, Ethernet 1000Base-T, obsługa PXE Boot
 |
| Gwarancja, Serwis, wsparcie techniczne producenta komputera | Firma serwisująca musi posiadać certyfikat ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokument potwierdzający należy załączyć do oferty.Serwis urządzeń musi być realizowany bezpośrednio przez Producenta lub przez serwis autoryzowany przez Producenta. Do oferty należy dołączyć oświadczenie podmiotu realizującego serwis lub producenta o spełnieniu w/w wymogu.Zamawiający wymaga od podmiotu realizującego serwis sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym gwarancją, uszkodzony dysk twardy pozostaje u Zamawiającego. * Minimum 3 lata gwarancji w trybie On-Site z gwarantowanym czasem reakcji serwisu w następnym dniu roboczym;
* Uszkodzone nośniki pozostają własnością Zamawiającego
* Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera
* Infolinia techniczna (wsparcia technicznego) producenta oferowanego komputera - dedykowana do rozwiązywania problemów technicznych dotyczących sprzętu i dostarczonego ze sprzętem oprogramowania – możliwość kontaktu przez telefon, formularz web oraz chat online, dostępna w dni powszednie od 9:00-18:00 w języku polskim – ogólnopolski numer stacjonarny bądź o ograniczonej odpłatności (0-800/801) – numer ten musi być powszechnie dostępnym numerem udostępnionym przez producenta sprzętu (nie może być to np. numer specjalnie uruchomiony na potrzeby niniejszego projektu). W ofercie należy podać numer telefonu. Zamawiający zachowuje sobie prawo weryfikacji możliwości obsługi technicznej poprzez kontakt na podany numer telefonu jako element oceny ofert);
* Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta jedynie poprzez podanie numeru seryjnego komputera;
 |