Załącznik nr 3 do SWZ-**zmieniony 15.10.2024**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Dostawa sprzętu infrastruktury IT w ramach projektu pn.: Cyberbezpieczny samorząd w Gminie Czersk” z podziałem na 9 części.**

**Zadanie jest dofinansowane w ramach Umowy o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0836/ FERC.02.02-CS.01-001/23/2024. Zadanie finansowane z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23.**

**Część 1 Dostawa serwerów – 3 sztuki**

1. **Serwer – 3 sztuki**

|  |  |
| --- | --- |
| Komponent | Minimalne wymagania |
| **Obudowa** | Obudowa typu Tower z możliwością instalacji do 8 dysków twardych 3,5”. |
| **Płyta główna** | Płyta główna z możliwością instalacji jednego fizycznego procesora, posiadająca minimum 4 sloty na pamięć RAM UDIMM, z możliwością zainstalowania do minimum 128GB pamięci RAM. Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym. |
| **Procesor** | Zainstalowany jeden procesor min. 8-rdzeniowy klasy x86, min. 2.8GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 90.9 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org |
| **Pamięć RAM** | 2x 32GB pamięci RAM UDIMM o częstotliwości taktowania minimum 4800MHz |
| **Funkcjonalność pamięci RAM** | Demand Scrubing,  Patrol Scrubing,  Permanent Fault Detection |
| **Sloty PCI Express** | minimum 4 sloty PCIe |
| **Interfejsy sieciowe/FC/SAS** | Minimum dwa interfejsy sieciowe 1Gb/s Ethernet nie zajmujące żadnego z dostępnych slotów PCIe |
| **Dyski twarde** | Zainstalowane:   * 2x dyski NLSAS o pojemności min. 4TB, Hot-Plug   Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10 |
| **Wbudowane porty** | Minimum 8 portów USB z czego min. 4 w technologii 3.0  1x RS-232  1x VGA |
| **Video** | Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1280x1024 pikseli |
| **Zasilanie** | Redundantne zasilacze o mocy 700W klasy Titanium |
| **Diagnostyka i Bezpieczeństwo** | * zintegrowany z płytą główną moduł TPM 2.0 * Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; * możliwość podmontowania zdalnych wirtualnych napędów; * wirtualną konsolę z dostępem do myszy, klawiatury; * wsparcie dla IPv6; * wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z Active Directory; * możliwość obsługi przez dwóch administratorów jednocześnie; * wsparcie dla dynamic DNS; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. * możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera * możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera   oraz z możliwością rozszerzenia funkcjonalności o:   * Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej * Przesyłanie danych telemetrycznych w czasie rzeczywistym * Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze * Automatyczna rejestracja certyfikatów (ACE) |
| **Oprogramowanie do zarządzania** | Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * integracja z Active Directory * Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish * Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram * Szczegółowy opis wykrytych systemów oraz ich komponentów * Możliwość eksportu raportu do CSV, HTML, XLS, PDF * Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. * Grupowanie urządzeń w oparciu o kryteria użytkownika * Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji * Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * Szybki podgląd stanu środowiska * Podsumowanie stanu dla każdego urządzenia * Szczegółowy status urządzenia/elementu/komponentu * Generowanie alertów przy zmianie stanu urządzenia. * Filtry raportów umożliwiające podgląd najważniejszych zdarzeń * Integracja z service desk producenta dostarczonej platformy sprzętowej * Możliwość przejęcia zdalnego pulpitu * Możliwość podmontowania wirtualnego napędu * Kreator umożliwiający dostosowanie akcji dla wybranych alertów * Możliwość importu plików MIB * Przesyłanie alertów „as-is” do innych konsol firm trzecich * Możliwość definiowania ról administratorów * Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów * Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta * Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów * Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. * Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. * Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile * Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. * Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. * Zdalne uruchamianie diagnostyki serwera. * Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. * Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001  Serwer musi posiadać deklaracja CE.  Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów, Microsoft Windows Server 2019, Microsoft Windows Server 2022. |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Warunki gwarancji** | Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat.  Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych)  Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.  Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.  Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.  Zamawiający wymaga **od Wykonawcy** dołączenia do oferty oświadczenia-potwierdzić w zał. nr 7 do SWZ, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   * Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. * Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. * Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. * Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. * Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.   Wymagane dołączenie do oferty **oświadczenia Wykonawcy** potwierdzić w zał. nr 7 potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń **– dokumenty potwierdzające należy załączyć do oferty.** |

1. **Oprogramowanie serwera – 3 sztuki**

1. Microsoft Windows Server Essential 2022 lub równoważne

Kryteria stosowane w celu oceny równoważności Microsoft Windows Server Essential 2022.

Przez oprogramowanie równoważne Zamawiający rozumie oprogramowanie spełniające następujące warunki poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

1. Obsługa do 64GB RAM
2. Obsługa do 10 rdzeni na serwerach z jednym gniazdem
3. Możliwość obsługi maksymalnie 25 użytkowników i 50 urządzeń
4. Oprogramowanie nie może wymagać dodatkowych licencji w celu uzyskania dostępu do serwera
5. Współpraca z procesorami o architekturze x86-64
6. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym
7. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory
8. Zawarta możliwość uruchomienia roli serwera DNS
9. Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP)
10. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory
11. Zawarta możliwość uruchomienia roli serwera stron WWW.

1. **Oprogramowanie serwera – 1 sztuka**

**Wymagane minimalne parametry**

Oprogramowanie Windows Server 2022 Standard lub równoważne.

Opis równoważności dla systemu Windows Server 2022 Standard:

1. System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji.
2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.
3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat.
4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego domeną Active Directory pracującą w oparciu o system Windows Server 2016 musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server
5. Licencja na system operacyjny musi być bez ograniczeń czasowych.
6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji.
7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
8. System operacyjny musi posiadać graficzny interfejs użytkownika.
9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:
10. zarządzania użytkownikami,
11. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,
12. możliwości przydzielania praw dostępu do zasobów sieciowych,
13. instalacji zdalnej oprogramowania z pakietów msi,
14. definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10,11.
15. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.
16. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Center.
17. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP.
18. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.
19. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.
20. System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra
21. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra
22. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.
23. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.
24. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
25. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
26. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
27. System operacyjny musi posiadać obsługa PowerShelI 5.1,
28. System operacyjny musi posiadać obsługa certyfikatów w Active Directory
29. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

**Część 2. Dostawa podzespołów do modernizacji serwerów.**

1. **Pamięć RAM – 6 sztuk**

|  |  |
| --- | --- |
| Minimalne wymagania: | |
| Pamięć wewnętrzna | min. 32 GB |
| Typ pamięci wewnętrznej | DDR4 RDIMM |
| Prędkość zegara pamięci | 2933 MHz |
| Korekcja ECC | Tak |
| Napięcie pamięci | 1.2 V |
| Moduł | 2Rx4 (Dual-Rank) |
| Złącze pamięci | 288-pin |
| Dodatkowe informacje | Pamięć wyprodukowana przez producenta serwera.  Dedykowana do serwera Dell PowerEdge T440 |

1. **Dyski twarde do posiadanego przez Zamawiającego serwera Dell PowerEdge R350.**
2. Dysk twardy – 1 sztuka

|  |  |
| --- | --- |
| Minimalne wymagania: | |
| Rodzaj urządzenia: | Dysk twardy Hot-Plug |
| Pojemność: | 4 TB |
| Rodzaj obudowy: | 3,5" |
| Interfejs: | NLSAS 12Gb/s |
| Szybkość transmisji urządzenia: | 1.2 GBps (zewnętrzna) |
| Prędkość obrotowa: | 7200 obr/min |
| Akcesoria w zestawie: | Półka na dyski |

1. Dysk twardy 1 sztuka

|  |  |
| --- | --- |
| Minimalne wymagania: | |
| Rodzaj urządzenia: | Dysk twardy Hot-Plug |
| Pojemność: | 600 GB |
| Rodzaj obudowy: | 2.5" w ramce 3.5" |
| Interfejs: | SAS 12Gb/s |
| Prędkość obrotowa: | 10000 obr/min |

1. **Komponenty serwera do posiadanego przez Zamawiającego serwera Dell PowerEdge T440.**

1. Dysk twardy – 1 sztuka.

|  |  |
| --- | --- |
| Minimalne wymagania: | |
| Rodzaj urządzenia: | Dysk twardy - Hot-Plug |
| Pojemność: | 8 TB |
| Rodzaj obudowy: | 3,5" |
| Interfejs: | NLSAS 12Gb/s |
| Prędkość obrotowa: | 7200 obr/min |
| Akcesoria w zestawie: | Półka na dyski |

1. 2 dyski M.2 **SATA** o pojemności min. 480GB z możliwością konfiguracji RAID 1 oraz kontrolerem BOSS.
2. Dysk twardy - 1 sztuka

|  |  |
| --- | --- |
| Minimalne wymagania: | |
| Rodzaj urządzenia: | Dysk twardy Hot-Plug |
| Pojemność: | 4 TB |
| Rodzaj obudowy: | 3,5" |
| Interfejs: | NLSAS 12Gb/s |
| Szybkość transmisji urządzenia: | 1.2 GBps (zewnętrzna) |
| Prędkość obrotowa: | 7200 obr/min |
| Akcesoria w zestawie: | Półka na dyski |

1. Dysk twardy - 1 sztuka

|  |  |
| --- | --- |
| Minimalne wymagania: | |
| Rodzaj urządzenia: | Dysk twardy Hot-Plug |
| Pojemność: | 600 GB |
| Rodzaj obudowy: | 2.5" w ramce 3.5" |
| Interfejs: | SAS 12Gb/s |
| Prędkość obrotowa: | 10000 obr/min |

1. Karta dual Port – 1 sztuka

|  |  |
| --- | --- |
| **Interfejsy sieciowe/FC/SAS** | * Dodatkowa karta Dual Port (2x SFP+, 10Gb/s, SFP+, PCIe) * 2x Okablowanie 2.0m **SEP+** |
| **Serwer** | * Dedykowana do posiadanego serwera T440 |

**Część 3 Dostawa serwerów NAS wraz z dyskami: 5 sztuk.**

1. **Serwer NAS – 5 sztuk**

|  |  |
| --- | --- |
| Typ urządzenia | Serwer NAS |
| Obudowa | Tower |
| Procesor | Czterordzeniowy procesor o taktowaniu 2.0 GHz (maksymalnie 2,7 GHz z przyspieszeniem) osiągający w teście PassMark co najmniej 2900 punktów |
| Sprzętowy mechanizm szyfrowania | Tak (AES-NI) |
| Pamięć RAM | min. 2 GB pamięci non-ECC SODIMM z możliwością rozszerzenia do min. 6 GB |
| Możliwości rozbudowy | * Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap * Wbudowane 2 gniazda M.2 obsługujące dyski NVMe. Dyski NVMe mogą posłużyć do utworzenia pamięć podręcznej bądź przestrzeni dyskowej |
| Porty zewnętrzne | Minimum:  • 2 porty USB 3.2.1 |
| Porty sieciowe | Minimum:  • 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) |
| Funkcja Wake on LAN/WAN | Tak |
| Wentylator obudowy | Min. 2 wentylatory 92 mm x 92 mm |
| Obsługiwane protokoły sieciowe | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |
| Obsługiwane systemy plików | Min.:  • Wewnętrzny: Btrfs, ext4  • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT |
| Zarządzanie pamięcią masową | • Maksymalny rozmiar pojedynczego wolumenu: 108 TB  • Minimalny liczba wewnętrznych wolumenów: 64  • Minimalny liczba obiektów iSCSI Target: 128  • Minimalny liczba jednostek iSCSI LUN: 256  • Obsługa klonowania/migawek jednostek iSCSI LUN |
| Obsługiwane typy macierzy RAID | Synology Hybrid RAID (SHR), Podstawowy (Basic), JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |
| Funkcja udostępniania plików | • Minimalna liczba kont użytkowników: 2048  • Minimalna liczba grup użytkowników: 256  • Minimalna liczba folderów współdzielonych: 512  • Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 500  • Minimalna liczba jednoczesnych połączeń protokołu SMB/AFP/FTP (z rozbudową pamięci RAM): 1500 |
| Uprawnienia | Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL) |
| Wirtualizacja | Obsługa VMware vSphere®, Citrix®, OpenStack® |
| Usługa katalogowa | Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP |
| Bezpieczeństwo | Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne  blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) |
| Obsługiwane systemy klienckie | Windows® 7 i nowsze, macOS® 10.12 i nowsze |
| Obsługiwane przeglądarki | Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach |
| Zasilanie | Wymogiem jest dostarczenie sprzętu wyposażonego w zasilacz maks. 90 W |
| Oprogramowanie | • Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych  • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów  • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.  • Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera  • pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia. |
| Gwarancja | Wykonawca udzieli gwarancji:  • 3 lat na urządzenia główne z możliwością przedłużenia do 5 lat za pomocą dodatkowego pakietu gwarancyjnego |

1. **Dyski twarde do serwera plików NAS z pozycji 1 części 3– 14 sztuk**

|  |  |
| --- | --- |
| Minimalne wymagania: | |
| Pojemność | min. 8000 GB |
| Typ | HDD (magnetyczny) |
| Format | Format 3,5 cala |
| Interfejs | Serial ATA III |
| Pamięć cache | min. 256 MB |
| Prędkość obrotowa | 7200 obr./ min. |

**Część 4 Dostawa zasilaczy awaryjnych.**

1. **UPS – 8 sztuk**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa elementu, parametru lub cechy** | **Opis wymagań** |
|  | Moc pozorna | 650 VA |
|  | Moc rzeczywista | 400 W |
|  | Układ zaawansowanej ochrony przeciwprzepięciowej (ASR) | Tak |
|  | Czas przełączenia na baterię | 5 ms |
|  | Liczba, typ gniazd wyj. z podtrzymaniem zasilania i ochroną przepięciową | 3 x FR |
|  | Liczba, typ gniazd wyj. z ochroną przepięciową | 1 x FR |
|  | Funkcja EcoControl | 1 gniazdo sterowane EcoControl (automatyczna dezaktywacja nieczynnych urządzeń peryferyjnych) |
|  | Typ gniazda wejściowego | IEC320 C14 (10A) |
|  | Czas podtrzymania dla obciążenia 70% | 5 min |
|  | Czas podtrzymania przy obciążeniu 50% | 9 min |
|  | Napięcie znamionowe wejściowego | 230 V |
|  | Tolerancja napięcia wejściowego | 184 V – 264 V (regulacja 161 V – 284 V) |
|  | Częstotliwość znamionowa | 50/60 Hz auto-selekcja |
|  | Tolerancja częstotliwości | 46 – 70 Hz |
|  | Napięcie znamionowe wyjściowe | 230 V (domyślnie), 220/240 V |
|  | Zakres zmian napięcia wyjściowego | +6/-10% napięcia nominalnego |
|  | Baterie wymieniane przez użytkownika | Tak |
|  | Baterie wewnętrzne o pojemności | 1 x 7Ah 12V |
|  | Porty komunikacji | USB, HID |
|  | Ochrona linii danych | Tel., Fax, Modem, Internet i Ethernet |
|  | Ochrona przepięciowa | Tak (zgodnie z  IEC 61643-1) 525 J |
|  | Panel sterowania diodowy | min. 2 diody LED |
| •  stan ostrzegawczy/awaria |
| •  stan przeciążenia na gniazdach z podtrzymaniem bateryjnym |
|  | Alarmy dźwiękowe | •  awaria UPSa |
| •  przeciążenie UPSa |
| •  niski stan naładowania baterii |
|  | Przyciski | •  Przycisk podświetlany ON/OFF LED załączania/ wyłączenia gniazd wyjściowych z podtrzymaniem bateryjnym |
|  | Kolor | Czarny |
|  | Typ obudowy | Uniwersalna Tower/Rack (możliwość instalacji pionowej, poziomej oraz w szafie Rack 19") |
|  | Wyposażenie standardowe | •  kabel USB |
| •  oprogramowanie na CD |
| •  1 x kabel zasilający zakończony wtykiem FR (PL) |
| •  instrukcja obsługi w języku polskim |
|  | Dołączone oprogramowanie | Do bezpiecznego zamykania systemów operacyjnych przy wyczerpaniu baterii kompatybilne z: Windows 7 / Vista/XP, Mac X OS, Linux |
|  | Maksymalna szerokość | 81 mm |
|  | Maksymalna wysokość | 263 mm |
|  | Maksymalna głębokość | 235 mm |
|  | Maksymalny ciężar | 3,6 kg |
|  | Cechy | Brak wentylatora, cicha praca, konstrukcja energooszczędna |
|  | Zimny start | Tak |
|  | Uruchomienie z baterii | Tak |
|  | Ochrona przed przeładowaniem | Tak |
|  | Gwarancja producenta 24 miesiące | Tak |
|  | Certyfikat CE | Tak |

1. **UPS – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa elementu, parametru lub cechy** | **Opis wymagań** |
| 1 | Moc pozorna | 3000VA |
| 2 | Moc rzeczywista | 3000W |
| 3 | Topologia (klasyfikacja IEC 62040-3) | Podwójna konwersja on-line z korekcją wejściowego współczynnika mocy systemu (PFC) |
| 4 | Sprawność przy pracy normalnej (100% obc.) | <94% |
| 5 | Sprawność w trybie podwyższonej sprawności (100% obc.) | >98% |
| 6 | Współczynnik mocy | 1 |
| 7 | Czas przełączenia na baterię | 0 ms |
| 8 | Możliwość pracy równoległej | tak |
| 9 | Liczba, typ gniazd wyjściowych | 8 gniazd IEC C13 (10A) + 2 gniazda IEC C19 (16A), w tym 2 zarządzalne grupy wraz z pomiarem zużytej energi |
| 10 | Typ gniazda wejściowego | 1 IEC C20 (16A) lub blok zacisków w wersji HotSwap MBP HW |
| 11 | Czas podtrzymania dla 100% obciążenia dla pf=1 | 3 min |
| 12 | Czas podtrzymania przy 50% obciążenia dla pf=1 | 10 min |
| 13 | Dodatkowe bateriie | Możliwość dołożenia maksymalnie 4 zewnętrznych modułow bateryjnych |
| 14 | Napięcie znamionowe | 200/208/220/230/240 V |
| 15 | Tolerancja napięci prostownika | 176V – 276 V (100-276V przy <33% obciążeniu) |
| 16 | Częstotliwość znamionowa | 50/60 Hz autodetekcja |
| 17 | Tolerancja częstotliwości | 40– 70 Hz |
| 18 | Kształt napięcia | Sinusoidalny |
| 19 | Napięcie znamionowe wyjściowe | 230 V (domyślnie) / możliwość wyboru 200/208/220/240 V |
| 20 | Zakres zmian napięcia | +/-1% napięcia nominalnego |
| 21 | Częstotliwość wyjściowa | 50/60 Hz +/-0,5% |
| 22 | Współczynnik szczytu | 3:1 |
| 23 | Dopuszczalny zakres współczynnika mocy obc. Liniowego | 0,5 indukcyjny - 0,5 pojemnościowy |
| 24 | Baterie wymieniane przez użytkownika "na gorąco" | Tak |
| 25 | Ochrona przed przeładowaniem | Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm) |
| 26 | Ochrona przed głębokim rozładowaniem | Tak |
| 27 | Okresowy automatyczny test baterii | Tak |
| 28 | System zarządzania pracą baterii | System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony. |
| 29 | Zdolność zwarciowa | 90A |
| 30 | Możliwość uruchomienia bez napięcia w sieci | Tak |
| 31 | Baterie wewnętrzne o pojemności nie mniejszej niż | 9Ah 12V, minimum 6 szt. |
| 32 | Czas ładowania baterii do poziomu 90% | < 1,5 godz. do 90% pojemności użytkowej |
| 33 | Interfejs komunikacyjny | •  USB |
| • RS232 DB-9 żeński (HID) |
| • 1 blok mini-zacisków dla zdalnego załączania/wyłączania |
| • 1 blok mini-zacisków do zdalnego wyłączania |
| • 1 blok mini-zacisków przekaźnika wyjściowego |
| 34 | Panel sterowania z wyświetlaczem LCD | • Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach.    Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe ,  częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny,napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii). |
| • Poziomy rząd przycisków sterowania |
| • Poziomy rząd wskaźników stanu : 4 LED |
| • Sygnalizator akustyczny |
| 35 | Sygnały akustyczne | • Awaria |
| • Niski stan naładowania baterii |
| • Przeciążenie |
| • Serwis |
| 36 | Przyciski sterujące i wskaźniki diodowe LED | • Przycisk Escape (anulowanie) |
| • Przyciski funkcyjne (przewijanie w górę i w dół) |
| • Przycisk Enter (potwierdzający) |
| • Przycisk ON/OFF załączenia i wyłączenia |
| • LED trybu zasilania z siec i(kolor zielony) |
| • LED trybu baterii (kolor żółty) |
| • LED usterki (kolor czerwony) |
| • LED w trybie obejścia (kolor pomarańczowy) |
| 37 | Kolor | Czarny RAL 9005 |
| 38 | Typ obudowy | Uniwersalna Tower/Rack 2U |
| 39 | Wyposażenie standardowe | UPS, instrukcja obsługi(CD), instrukcja bezpieczeństwa, instrukcja szybkiego montażu |
| 1 x kabel szeregowy RS-232, |
| 1 x kabel komunikacyjny USB |
| 1 x kable wyjściowe IEC 16A |
| 2 x kable wyjściowe IEC 10A |
| uchwyty kablowe |
| 1 x zestaw szyn montażowych 19’ |
| podstawki do montażu wieżowego |
| 40 | Dołączone oprogramowanie | Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów zasilanych z systemu i pracujących pod kontrolą systemów operacyjnych:    - Windows:     7 / 8 / 2008 / Vista / 2003 / XP   - Microsoft SCVMM 2012   - Linux:   Debian GNU Linux: Lenny,   SUSE/Novell: SLES 11, OpenSUSE 11.2,    Redhat Enterprise Linux: RHEL 5.3, 5.4, 5.5, Fedora core 12    Ubuntu: 10.04   - VMWare: vCenter / ESXi 5.1    - Citrix XEN 6.0 |
| 41 | Zgodność ze standardem Energy Star | Tak |
| 42 | Maksymalna szerokość | 440 mm |
| 43 | Maksymalna wysokość | 86,5 mm |
| 44 | Maksymalna głębokość | 605 mm |
| 45 | Maksymalny ciężar | 27,4 kg |
| 46 | Poziom hałasu w odl. 1m | <47 dBA dla pracy normalnej |
| 47 | Znaki bezpieczeństwa | CE, C-Tick, IEC/EN 62040-1, IEC/EN 62040-2: Kat. C1, IEC/EN 62040-3 |
| 48 | Gwarancja producenta | 3 lata na elektronikę, 2 lata na baterie akumulatorów |

1. **UPS – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa elementu, parametru lub cechy | Opis wymagań |
| 1 | Moc pozorna | 2200 VA |
| 2 | Moc rzeczywista | 1980 W |
| 3 | Topologia  (klasyfikacja IEC 62040-3) | Line-interactive z AVR |
| 4 | Współczynnik mocy | 0,9 |
| 5 | Czas przełączenia na baterię | <4 ms |
| 6 | Liczba, typ gniazd wyjściowych | 8 x IEC C13 oraz 1 x IEC C19 16A |
| 7 | Typ gniazda wejściowego | IEC C20 16A |
| 8 | Czas podtrzymania dla 100% obciążenia dla pf=0,9 | 2 min |
| 9 | Czas podtrzymania przy 50% obciążenia dla pf=0,9 | 7 min |
| 11 | Napięcie znamionowe | 200/208/220/230/240/250 V |
| 12 | Tolerancja napięci prostownika | 184V - 276V |
| 13 | Częstotliwość znamionowa | 50/60 Hz autodetekcja |
| 14 | Tolerancja częstotliwości | 45– 55 Hz (sieć 50 Hz) 55 - 65 (sieć 60Hz) |
| 15 | Kształt napięcia | Sinusoidalny |
| 16 | Napięcie znamionowe wyjściowe | 220/230/240 V do wyboru przez użytkownika |
| 17 | Zakres zmian napięcia | +6/-10% napięcia nominalnego |
| 18 | Częstotliwość wyjściowa | 50/60 Hz |
| 19 | Współczynnik szczytu | 3:1 |
| 20 | Baterie wymieniane przez użytkownika "na gorąco" | Tak |
| 21 | Ochrona przed przeładowaniem | Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm) |
| 22 | Ochrona przed głębokim rozładowaniem | Tak |
| 23 | Okresowy automatyczny test baterii | Tak |
| 24 | System zarządzania pracą baterii | System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony. |
| 26 | Możliwość uruchomienia bez napięcia w sieci | Tak |
| 27 | Baterie wewnętrzne o pojemności nie mniejszej niż | 9Ah 12V, minimum 4 szt. |
| 28 | Czas ładowania baterii do poziomu 90% | < 3 godz. do 90% pojemności użytkowej |
| 29 | Interfejs komunikacyjny | •  USB |
| • RS232 DB-9 żeński (HID) |
| • port ROO oraz RPO |
| 30 | Panel sterowania z wyświetlaczem LCD | • Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. |
| • Poziomy rząd przycisków sterowania |
| • Poziomy rząd wskaźników stanu : zasialanie z siec(zielony), trybu bateryjnego (żółty), usterki (czerwony) |
| • Sygnalizator akustyczny |
| 31 | Sygnały akustyczne | • Awaria |
| • Niski stan naładowania baterii |
| • Przeciążenie |
| • Serwis |
| 32 | Przyciski sterujące i wskaźniki diodowe LED | • Przycisk Escape (anulowanie) |
| • Przyciski funkcyjne (przewijanie w górę i w dół) |
| • Przycisk Enter (potwierdzający) |
| • Przycisk ON/OFF załączenia i wyłączenia |
| • LED trybu zasilania z siec i(kolor zielony) |
| • LED trybu baterii (kolor żółty) |
| • LED usterki (kolor czerwony) |
| 33 | Kolor | Czarny RAL 9023 / RAL 9005 |
| 34 | Typ obudowy | Uniwersalna Tower/Rack 2U |
| 35 | Wyposażenie standardowe | UPS, instrukcja obsługi(CD), instrukcja bezpieczeństwa |
| 1 x kabel szeregowy RS-232, |
| 1 x kabel komunikacyjny USB |
| 2 x kable wyjściowe IEC 10A |
| 2 x uchwyty kablowe |
| 1 x zestaw szyn montażowych 19’ |
| 1x kabel wejściowy |
| 38 | Maksymalna szerokość | 441 mm |
| 39 | Maksymalna wysokość | 86,5 mm |
| 40 | Maksymalna głębokość | 552 mm |
| 41 | Maksymalny ciężar | 27 kg |
| 42 | Poziom hałasu w odl. 1m | do 45 dBA dla pracy normalnej |
| 43 | Znaki bezpieczeństwa | CE, IEC/EN 62040-1 (CB Report), IEC/EN 62040-2 class B |
| 44 | Gwarancja producenta | 24 miesiące |
| 45 | Możliwość montażu ręcznego bypassu serwisowego | Tak |

**Część 5 Dostawa urządzeń sieciowych.**

1. **Zarządzane urządzenia sieciowe z obsługą VLAN – 8 sztuk**

Urządzenie powinno być objęte ograniczoną wieczystą gwarancją producenta trwającą 5 lat.

Konfiguracja przełącznika oraz wymagane funkcje.

* 8 x 1Gb/s
* MTBF min. 1638156 godzin
* Bufor pakietów min.: 192KB
* Przepustowość min.: 16 Gbps
* Kolejkowanie Weighted Round Robin (WRR), Strict Priority
* Ilość obsługiwanych VLAN min. 32
* IGMP snooping ver. 1, 2, 3
* Obsługa CoS
* Port Mirroring
* Test okablowania

Certyfikaty bezpieczeństwa oraz elektromagnetyczne

* CE mark, commercial
* FCC Part 15 class B
* CE/EN55032/24
* VCCI
* ACMA

1. **Zarządzane urządzenia sieciowe z obsługą VLAN – 2 sztuki**

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

* Ilość portów 8 portów SFP+ oraz 8 portów 10GBaseT niezależne
* Chłodzenie od przedu do tyłu obudowy
* Tablica MAC min. 16K
* Tablica ARP/NDP min. 888
* Bufor 16Mb
* MTBF min. 196120 godzin
* Wydajność min. 238 Mp/s
* Przepustowość min. 320 Gb/s
* Port USB
* Port miniUSB
* Port zarządzania Out-of-band;
* Web GUI
* HTTPs
* CLI
* Telnet
* SSH
* SNMP
* MIB RSPAN
* Radius
* TACACS+
* DiffServ
* Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
* IPv4/IPv6 Multicast filtering
* IGMPv3 MLDv2 Snooping
* ASM & SSM
* IGMPv1,v2 Querier
* Auto-VoIP
* Auto-iSCSI
* Policy-based routing (PBR)
* LLDP-MED
* Spanning Tree
* Green Ethernet
* STP
* MTP
* RSTP
* PV(R)STP
* BPDU/STRG Root Guard
* EEE (802.3az)
* GVRP/GMRP
* Q in Q,
* Private VLAN
* DOT1X
* MAB
* Captive Portal
* DHCP Snooping
* Dynamic ARP
* Inspection
* IP Source Guard
* CPU min 800 Mhz
* Min 1GB RAM
* Min 256MB Flash
* Min ilość obsługiwanych VLAN 4K
* DHCP Server min 2K rezerwacji
* sFlow
* Minimalna ilość przełączników w stosie: 8
* Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s
* Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
* Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
* Non-stop forwarding (NSF)
* Distributed Link Aggregation (LAGs across the stack)
* Ilość interfejsów IP 128
* Double VLAN Tagging (QoQ)
* Yes
* PIM-DM (Multicast Routing - dense mode)
* PIM-DM (IPv6)
* PIM-SM (Multicast Routing - sparse mode)
* PIM-SM (IPv6)
* RIPv1
* RIPv2
* OSPFv2
* RFC 2328
* RFC 1583
* OSPFv3
* OSPFv2 min. sąsiadów 400
* OSPFv3 min. sąsiadów 400
* OSPFv3 min. sąsiadów na interfejs 100
* UDLD
* LLPF
* DHCPv6 Snooping
* wysyłanie alertów na email
* MMRP
* Ilość ACL min. 100
* Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu

1. **Zarządzane urządzenia sieciowe z obsługą VLAN – 2 sztuki**

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

* Ilość portów 48 porty PoE+ 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne
* Chłodzenie od przodu do tyłu obudowy
* Budżet mocy PoE min.: 832W oraz zasilacz o mocy 1000W
* Możliwość instalacji redundantnego zasilacza
* Tablica MAC min. 16K
* Tablica ARP/NDP min. 888
* Bufor 16Mb
* MTBF min. 673207 godzin
* Wydajność min. 130,9 Mp/s
* Przepustowość min. 176 Gb/s
* Port USB
* Port miniUSB
* Port zarządzania Out-of-band;
* Web GUI
* HTTPs
* SSH
* SNMP
* MIB RSPAN
* Radius
* TACACS+
* DiffServ
* Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
* IPv4/IPv6 Multicast filtering
* CPU min 800 Mhz
* Min 1GB RAM
* Min 256MB Flash
* Min ilość obsługiwanych VLAN 4K
* Minimalna ilość przełączników w stosie: 8
* Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
* Możliwość łączenia przełączników w stos w konfiguracji: spine and leaf
* Non-stop forwarding (NSF)
* Distributed Link Aggregation (LAGs across the stack)
* Double VLAN Tagging (QoQ)
* PIM-DM (Multicast Routing - dense mode)
* PIM-DM (IPv6)
* PIM-SM (Multicast Routing - sparse mode)
* PIM-SM (IPv6)
* RIPv1
* RIPv2
* OSPFv2
* RFC 2328
* RFC 1583
* OSPFv3
* CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014,
* Class A, EN 61000-3-3:2013, EN 55024:2010
* VCCI : VCCI-CISPR 32:2016, Class A
* RCM: AS/NZS CISPR 32:2013 Class A
* FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014
* ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014
* BSMI: CNS 13438 Class A
* CB report / certificate IEC 60950-1:2005 (ed.2)+A1:2009+A2:2013
* UL listed (UL 1950)/cUL IEC 950/EN 60950
* CE LVD: EN 60950-1: 2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013
* RCM (AS/NZS) 60950.1:2015

**Część 6 Dostawa serwera: 1 sztuka.**

1. **Serwer – 1 sztuka**

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | * Obudowa Rack o wysokości max 2U z możliwością instalacji min. 8 dysków 3.5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. * Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. * Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| **Płyta główna** | * Płyta główna z możliwością zainstalowania do dwóch procesorów. * Obsługa procesorów 32 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinno znajdować się minimum 16 sloty przeznaczone do instalacji pamięci. * Płyta główna powinna obsługiwać do 1TB pamięci RAM. |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | * Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86, min. 2.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 265 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| **RAM** | * Minimum 256GB DDR5 RDIMM 4800MT/s, |
| **Funkcjonalność pamięci RAM** | * Demand Scrubbing, * Patrol Scrubbing, * Permanent Fault Detection (PFD) |
| **Gniazda PCI** | * Min. dwa sloty PCIe |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT * 2 x SFP28, 25 Gb/s, SFP28, OCP 3.0 **na karcie PCIe** |
| **Dyski twarde** | Zainstalowane:   * 2 dyski HDD NLSAS o pojemności min. 8TB, Hot-Plug. * 2 dyski M.2 NVME o pojemności min. 480GB z możliwością konfiguracji RAID 1. |
| **Kontroler RAID** | * Sprzętowy kontroler dyskowy, posiadający * Min. 8GB nieulotnej pamięci cache, * Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.   Wsparcie dla dysków samoszyfrujących. |
| **Wbudowane porty** | * 4x USB, w tym min. 1 porty USB 3.0 * 2x port VGA (jeden na panelu przednim) * Możliwość rozbudowy o Serial Port |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |
| **Wentylatory** | * Redundantne, Hot-Plug |
| **Zasilacze** | * Redundantne, Hot-Plug min. 1100W klasy Titanium |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem * Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| **Karta Zarządzania** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   + zdalny dostęp do graficznego interfejsu Web karty zarządzającej;   + zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);   + szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;   + możliwość podmontowania zdalnych wirtualnych napędów;   + wirtualną konsolę z dostępem do myszy, klawiatury;   + wsparcie dla IPv6;   + wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;   + integracja z Active Directory;   + możliwość obsługi przez dwóch administratorów jednocześnie;   + wsparcie dla dynamic DNS;   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.   + możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera   + możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera   oraz z możliwością rozszerzenia funkcjonalności o:   * + Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej   + Przesyłanie danych telemetrycznych w czasie rzeczywistym   + Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze   + Automatyczna rejestracja certyfikatów (ACE) |
| **Oprogramowanie do zarządzania** | * Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   + Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych   + integracja z Active Directory   + Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta   + Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish   + Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram   + Szczegółowy opis wykrytych systemów oraz ich komponentów   + Możliwość eksportu raportu do CSV, HTML, XLS, PDF   + Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.   + Grupowanie urządzeń w oparciu o kryteria użytkownika   + Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji   + Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach   + Szybki podgląd stanu środowiska   + Podsumowanie stanu dla każdego urządzenia   + Szczegółowy status urządzenia/elementu/komponentu   + Generowanie alertów przy zmianie stanu urządzenia.   + Filtry raportów umożliwiające podgląd najważniejszych zdarzeń   + Integracja z service desk producenta dostarczonej platformy sprzętowej   + Możliwość przejęcia zdalnego pulpitu   + Możliwość podmontowania wirtualnego napędu   + Kreator umożliwiający dostosowanie akcji dla wybranych alertów   + Możliwość importu plików MIB   + Przesyłanie alertów „as-is” do innych konsol firm trzecich   + Możliwość definiowania ról administratorów   + Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów   + Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)   + Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta   + Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów   + Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.   + Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.   + Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile   + Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera.   + Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.   + Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * Serwer musi posiadać deklaracja CE. * Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Warunki gwarancji** | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. * Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. * Zamawiający wymaga od Wykonawcy dołączenia do oferty oświadczenia potwierdzić w zał. nr 7, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   + Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.   + Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.   + Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.   + Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Wymagane dołączenie do oferty oświadczenia **Wykonawcy** potwierdzić w zał. nr 7 potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta **urządzeń – dokumenty potwierdzające należy załączyć do oferty.** |

1. **Oprogramowanie serwera – 55 sztuk**

1. Licencje dostępowe na użytkownika

* Wymagana licencja typu Cal User OEM do systemu Windows Server 2022 (z niniejszego zamówienia) lub równoważne, jeśli oprogramowanie równoważne takich licencji wymaga.

1. Opis równoważności dla funkcjonalności dotyczące wymaganego przez Zamawiającego oprogramowania równoważnego do Windows Server 2022 na użytkownika:

* Licencja dostępowa dla użytkownika umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2022 typu User Cal z wdrożoną rolą Active Directory

1. **Oprogramowanie serwera – 2 sztuki**

Licencje systemu operacyjnego Microsoft Windows Server 2022 Datacenter 16-core lub oprogramowania równoważnego nie mogą posiadać ograniczeń czasowych, muszą pochodzić z oficjalnego kanału dystrybucji. Licencje nie mogą być dedykowane tylko do jednego producenta sprzętu serwerowego.

**RÓWNOWAŻNOŚĆ:**

**1. Warunki równoważności dla licencji systemu Microsoft Windows Server 2022 Datacenter.**

W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2022 Datacenter. Zamawiający wymaga, aby produkt równoważny spełniał niżej wymienione wymagania:

1. Współpraca z procesorami o architekturze x86 – 64bit.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 16 rdzeni.
5. Praca w roli klienta domeny Microsoft Active Directory.
6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016.
7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
11. Możliwość uruchomienia roli serwera stron WWW.
12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
18. pozwalają na zmianę rozmiaru w czasie pracy systemu,
19. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
20. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
21. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
22. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość
23. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
24. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
25. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
26. Możliwość wykorzystania standardu http/2.
27. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
28. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
29. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
30. Mechanizmy logowania w oparciu o: a) login i hasło,
31. karty z certyfikatami (smartcard),
32. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
33. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
34. określonych grup użytkowników,
35. zastosowanej klasyfikacji danych,
36. centralnych polityk dostępu w sieci,
37. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
38. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
39. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
40. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
41. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji    
    w dokumentach (Digital Rights Management).
42. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
43. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
44. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
45. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

* podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
* ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
* odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
* bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.,

1. zdalna dystrybucja oprogramowania na stacje robocze,
2. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,
3. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

* Dystrybucję certyfikatów poprzez http,
* Konsolidację CA dla wielu lasów domeny,
* Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
* Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

1. szyfrowanie plików i folderów,
2. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
3. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
4. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
5. serwis udostępniania stron WWW,
6. wsparcie dla protokołu IP w wersji 6 (IPv6),
7. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
8. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
9. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
10. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover    
    z jednoczesnym zachowaniem pozostałej funkcjonalności.
11. mechanizmy wirtualizacji mające wsparcie dla:

* dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
* obsługi ramek typu jumbo frames dla maszyn wirtualnych.
* obsługi 4-KB sektorów dysków,
* nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
* możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.

1. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
2. wsparcie dla rozwiązania Kubernetes.
3. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz    
   z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
4. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
5. mechanizmy deduplikacji i kompresji na wolumenach.
6. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
7. mechanizm konfiguracji połączenia VPN do platformy Azure.
8. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
9. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
10. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).

**Część 7 Dostawa macierzy dyskowej.**

1. **Macierz dyskowa – 1 sztuka**

|  |  |
| --- | --- |
| **Element konfiguracji/cecha/funkcjonalność** | **Wymagania minimalne** |
| Typ obudowy | Macierz musi być przystosowana do montażu w szafie rack 19”,    o wysokość maksymalnie 2U oraz umożliwiać montaż min. 12 dysków 3.5” |
| Przestrzeń dyskowa | Zainstalowane:  6x dysk HDD SAS o pojemności min. 2.4TB, Hot-Plug  6x dysk HDD NLSAS o pojemności min. 16TB, Hot-Plug |
| Możliwość rozbudowy | Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardych. |
| Obsługa dysków | Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. |
| Sposób zabezpieczenia danych | Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).  Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID.  Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).  Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków. |
| Tryb pracy kontrolerów macierzowych | Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów. |
| Pamięć cache | Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.  Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.  Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat. |
| Rozbudowa pamięci cache | Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem. |
| Interfejsy | Macierz musi posiadać, co najmniej 8 portów iSCSI 25Gb (4 porty na kontroler), |
| Kable/wkładki | 4x kabel DAC 25GbE SFP28-SFP28 min. 5m |
| Zarządzanie | Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. |
| Zarządzanie grupami dyskowymi oraz dyskami logicznymi | Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej.  Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Thin Provisioning | Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.  Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Tiering | Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.  Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.  Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych. |
| Wewnętrzne kopie migawkowe | Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.  Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Wewnętrzne kopie pełne | Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Migracja danych w obrębie macierzy | Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia. |
| Zdalna replikacja danych | Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem. |
| Podłączanie zewnętrznych systemów operacyjnych | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).  Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.  Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie. |
| Redundancja | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.  Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.  Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.  Zasilacze użyte w macierzy powinny posiadać certyfikat sprawności zasilacza minimum 80+ Gold. |
| Dodatkowe wymagania | Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.  Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie. |
| Standardy bezpieczeństwa | Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International) |
| Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym  producenta. Na żądanie Zamawiającego, Wykonawca musi  przedstawić oświadczenie producenta oferowanego serwera,  potwierdzające pochodzenie urządzenia z oficjalnego kanału  dystrybucyjnego producenta.  Wymagane są dokumenty poświadczające, że sprzęt jest  produkowany zgodnie z normami ISO 9001 oraz ISO 14001.  Deklaracja zgodności CE. |
| Warunki gwarancji | 5 lat gwarancji producenta  Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych.  Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.  Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.  Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.  Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.  Zamawiający wymaga od Wykonawcy dołączenia do oferty oświadczenia potwierdzić w zał. nr 7, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Możliwość rozszerzenia gwarancji przez producenta do 7 lat.  **Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.**  Wymagane dołączenie do oferty oświadczenia Wykonawcy potwierdzić w zał. nr 7 potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. |

**Część 8 Dostawa oprogramowania.**

1. **Licencje UTM – 1 sztuka**

Przedłużenie licencji do posiadanego przez Zamawiającego urządzenia UTM Stormshield SN310 Premium UTM Security Pack  na 12 miesięcy.

1. **Oprogramowanie antywirusowe**

Oprogramowanie antywirusowe - okres ochrony: 2 lata, liczba stanowisk: 7

**Ochrona stacji roboczych - Windows**

1. Pełne wsparcie dla systemu Windows 10/Windows 11.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
4. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
5. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim oraz angielskim.

**Ochrona antywirusowa i antyspyware**

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
7. System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
9. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
13. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
14. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
15. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
16. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
17. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
18. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
19. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
20. Wbudowany konektor dla programów MS Outlook.
21. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
22. 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).
23. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
24. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
25. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
26. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
27. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
28. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
29. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
30. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
31. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
32. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
33. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
34. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
35. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
36. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
37. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
38. Możliwość automatycznego wysyłania nowych do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
39. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
40. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
41. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
42. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
43. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
44. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
45. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
46. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
47. Program ma umożliwiać 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.
48. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
49. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
50. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
51. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
52. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
53. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
54. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

* tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
* tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
* tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
* tryb uczenia się, w którym program 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,
* tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

1. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
2. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
3. Aplikacja musi posiadać dedykowaną funkcję, wykorzystującą technologię procesorów Intel (TDT) w zakresie zwiększenia skuteczności wykrywania zagrożeń wymuszających okup.
4. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
5. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
6. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
7. Funkcja, generująca taki log, ma posiadać przynajmniej 3 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
8. Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
9. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
10. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
11. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
12. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
13. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
14. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
15. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
16. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
17. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli rodzicielskiej i kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
18. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
19. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
20. Możliwość podejrzenia informacji o licencji, która znajduje się w programie.
21. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
22. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
23. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
24. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
25. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.
26. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
27. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
28. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
29. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
30. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

**Ochrona przed spamem**

1. Ochrona antyspamowa dla programów pocztowych MS Outlook.
2. Program ma umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
3. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
4. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
5. Możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
6. Możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
7. Możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
8. Program ma domyślnie współpracować z folderem „Wiadomości-śmieci”, dostępnym w programie Microsoft Outlook.
9. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana”
10. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana”.
11. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

**Zapora osobista (personal firewall)**

1. Zapora osobista ma pracować w jednym z czterech trybów:

* tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
* tryb interaktywny – program pyta się o każde nowo nawiązywane połączenie,
* tryb oparty na regułach – program blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
* tryb uczenia się – program automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

1. Program musi oceniać reguły zapory systemu Windows. 105. Możliwość tworzenia list sieci zaufanych.
2. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
3. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
4. Możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
5. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
6. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
7. Wykrywanie modyfikacji w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
8. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
9. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
10. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
11. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
12. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
13. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
14. Program musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów: z aplikacją lokalną, którą administrator wskazuje z listy, z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.

**Kontrola rodzicielska**

1. Aplikacja musi być wyposażona w zintegrowany moduł kontroli rodzicielskiej.
2. Moduł Kontroli rodzicielskiej musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane reguły filtrowania.
3. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
4. Dla kont użytkowników musi istnieć możliwość przypisania gotowych profili filtrowania kategorii.
5. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
6. Podstawowe kategorie, w jakie aplikacja musi być co najmniej wyposażona to: Osoby dorosłe, Agresywne, Alkohol i wyroby tytoniowe, Ukrywające tożsamość, Sztuka, Motoryzacja, Biznes i praca, Czaty i sieci społecznościowe, komunikacja, Działalność przestępcza, Oświata, Rodzina i wychowanie dzieci, Moda, Finanse, Żywność i napoje, Zdrowie, Hobby i zainteresowania, Dzieci, Styl życia, Aktualności, Zwierzęta domowe, Zagadnienia społeczne, polityczne i prawne, Nieruchomości, Religia, Nauka, Edukacja seksualna, Zakupy, Sport, Technologie, Podróże
7. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.
8. Dla poszczególnych kont użytkownik ma posiadać możliwość utworzenia wyjątków dla konkretnych adresów url, które mogą być wyświetlone nawet w przypadku, gdy dany adres znajduje się w którejkolwiek z blokowanych kategorii.
9. Aplikacja musi być wyposażona w moduł logowania zablokowanych stron oraz kategorii niezależnie od zalogowanego użytkownika.
10. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli rodzicielskiej.

**Ochrona Bankowości elektronicznej**

1. Aplikacja musi być wyposażona w moduł ochrony bankowości internetowej.
2. Przeglądarka powinna automatycznie szyfrować wszelkie dane wpisywane przez Użytkownika w formularzach internetowych. Szyfrowanie powinno odbywać się na poziomie odczytu znaków wpisywanych z klawiatury.
3. Użytkownik w każdym czasie musi mieć możliwość ręcznego uruchomienia przeglądarki w trybie zabezpieczonym modułem ochrony bankowości elektronicznej dla dowolnego adresu URL.
4. Praca w trybie bezpiecznym musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na pasku przeglądarki.

**Monitor sieci domowej**

1. Aplikacja ma posiadać moduł skanujący sieć domową, do której podłączony jest użytkownik, wyświetlając obecnie podłączone urządzenia sieciowe oraz sygnalizować nowo podłączane.
2. Wyświetlane hosty widoczne są pod ich nazwą NETBIOS, adresem IP oraz adresem MAC. Wraz z tymi informacjami wyświetlane muszą być informacje na temat ostatniego wykrycia hosta.
3. Wyświetlana nazwa hosta może być modyfikowana przez użytkownika.
4. Aplikacja musi być wyposażona w mechanizm umożliwiający tworzenie reguł dla ostatnio zablokowanej komunikacji, użytkownik musi mieć możliwość wyświetlania komunikacji, jaka była blokowana w ostatnim czasie (co najmniej ostanie 5,15,60 minut).
5. Użytkownik ma możliwość otwarcia interfejsu logowania się do swojego urządzenia brzegowego (routera itp.) poprzez link umieszczony w menu aplikacji.
6. Moduł ochrony sieci musi mieć możliwość przeprowadzenia audytu zabezpieczeń routera znajdującego się w sieci użytkownika.
7. System skanowania routera musi mieć możliwość wykrycia co najmniej otwartych portów sieciowych, zabezpieczenia konfiguracji urządzenia za pomocą domyślnych lub słabych haseł.
8. Moduł ochrony sieci domowej wykonujący skanowanie pod kątem otwartych portów powinien sprawdzać co najmniej porty 80, 443, 139, 445, 21, 22, 23.
9. Moduł musi wykrywać również urządzenia podłączone w sieci domowej należące do grupy produktów „Internet of Things”.
10. Moduł ten musi mieć możliwość wykrycia, czy urządzenie pracuje w sieci publicznej czy lokalnej. W przypadku sieci publicznej program musi wyświetlić ostrzeżenie użytkownikowi o ryzyku skanowania w takim trybie.

**Ochrona kamery internetowej**

1. Aplikacja ma umożliwiać kontrolę użycia kamery internetowej przez procesy znajdujące się w systemie jak i inne aplikacje.
2. W przypadku próby użycia kamery przez aplikację lub proces systemowy, użytkownikowi musi wyświetlić się stosowny komunikat ostrzegawczy.
3. Wykrycie próby użycia kamery musi dać użytkownikowi możliwość zezwolenia lub blokady takiej czynności.
4. Użytkownik może utworzyć listę aplikacji, które będą miały dostęp do kamery. Analogiczna lista musi zostać utworzona dla aplikacji, dla których wykonywana będzie blokada.

**Ochrona antykradzieżowa**

1. Program musi posiadać moduł umożliwiający powiązanie zainstalowanego w systemie pakietu ochrony z kontem utworzonym na dedykowanym serwisie online dostępnym za pomocą przeglądarki internetowej na serwerach producenta.
2. Po zalogowaniu do swojego indywidualnego konta na portalu producenta użytkownik powinien mieć wylistowane urządzenia, z którymi jest to konto powiązane.
3. Logowanie do portalu za pomocą przeglądarki internetowej musi odbywać się poprzez zabezpieczoną komunikację HTTPS.
4. Portal musi posiadać polski interfejs.
5. Użytkownik z poziomu swojego konta musi posiadać możliwość wykonania testu na widocznym w portalu swoim komputerze w celu weryfikacji poprawności działania modułu antykradzieżowego.
6. Wyzwolenie zadania testu musi wymagać potwierdzenia jego wykonania od strony użytkownika urządzenia, na którym test ma być wykonany.
7. W trakcie testu mechanizmy wbudowane w pakiet antywirusowy muszą zebrać co najmniej informację o: lokalizacji testowanego komputera ( jeśli jest ona dostępna ) – urządzenie powinno być wskazane na mapie w postaci graficznej, wykonać screenshoot’a pulpitu oraz wykonać zdjęcie za pomocą wbudowanej w komputer kamery (jeśli jest dostępna) i zebrać informację o adresie IP, z jakiego łączy się testowany komputer.
8. Zebrane podczas testów informacje muszą być widoczne dla zalogowanego na portalu użytkownika.
9. W przypadku kradzieży lub zagubienia urządzenia, Użytkownik musi posiadać możliwość określenia swojego urządzenia jako brakującego.
10. W momencie, gdy urządzenie zostanie określone jako brakujące, automatycznie musi zostać przesłane na nie zadanie aktywacji dedykowanego konta systemowego z ograniczeniami, oraz wymuszenie restartu systemu Windows.
11. Po restarcie komputera musi istnieć możliwość zalogowania się jedynie do konta z ograniczeniami utworzonego przez mechanizmy auto ochrony, pozostałe konta systemowe mają być nieaktywne.
12. Mechanizm antykradzieżowy w momencie aktywacji ma automatycznie tworzyć zdjęcia przy wykorzystaniu wbudowanej w urządzenie kamery (jeśli dostępna), zapisywać obraz pulpitu, zbierać informacje odnośnie lokalizacji urządzenia oraz wykorzystywanych adresów IP.
13. Zebrane informacje mają zostać przesłane na konto użytkownika utworzone na portalu producenta.
14. W przypadku braku połączenia z siecią Internet, w/w informacje maja być zbierane i przesłane do portalu w momencie, gdy urządzenie będzie posiadało aktywne połączenie z siecią Internet.
15. Zalogowany do konta na portalu producenta użytkownik musi posiadać możliwość zdalnego wyświetlenia na brakującym urządzeniu dowolnego komunikatu zawierającego tekst i obraz.
16. Z poziomu portalu, użytkownik musi mieć dostęp do danych historycznych wcześniej zebranych podczas testów lub w momencie określenia urządzenia jako brakującego.
17. Użytkownik musi posiadać opcję usunięcia swojego konta z serwerów producenta wraz z informacjami tam się znajdującymi.

**Menedżer licencji**

1. Interfejs menedżera licencji musi być dostępny z poziomu strony WWW.
2. Dostęp do witryny musi być zabezpieczony z pomocą SSL.
3. Interfejs webowy musi być dostępny w języku polskim.
4. Interfejs www musi posiadać możliwość dodania więcej niż jednej licencji.
5. Produkt zabezpieczający musi posiadać możliwość aktywacji przy pomocy danych logowania menedżera licencji.
6. Komputer po aktywacji musi się zgłaszać do menedżera licencji za pomocą nazwy NETBIOS.
7. Menedżer musi pokazywać liczbę wykorzystanych i dostępnych licencji.
8. Musi być możliwość zmiany nazwy komputera na stornie www po dokonaniu aktywacji .
9. Dezaktywacja licencji musi być dostępna bezpośrednio z interfejsu www.
10. Przy usuwaniu licencji z interfejsu www musi być dostępna opcja dezaktywacji wszystkich stacji.

**Prywatność i zabezpieczenia przeglądarki**

1. Czyszczenie danych przeglądarki musi być obsługiwane przez rozszerzenie instalowane bezpośrednio w przeglądarkach Google Chrome, Mozilla Firefox oraz Microsoft Edge.
2. Produkt musi pozwalać na usuwanie danych przeglądarki, minimum: historia pobierania, historia przeglądania, pliki cookie, obrazy i pliki zapisane w pamięci podręcznej, hasła i dane logowania, autouzupełnianie danych formularzy.
3. Produkt musi zezwalać na tworzenie listy stron internetowych, których czyszczenie danych przeglądarki nie dotyczy.
4. Produkt musi pozwalać na czyszczenie w trybie jednorazowym bądź cyklicznym.
5. Produkt musi posiadać funkcjonalność skanującą wyniki wyszukiwania i wyświetlać informacje o tym czy witryna jest bezpieczna.

**Sandbox w chmurze**

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
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.
4. Użytkownik musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Użytkownik musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Użytkownik musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
8. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej.

W przypadku wykrycia zagrożenia, komputer jest bezzwłocznie chroniony.

1. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

**Menadżer haseł**

1. Produkt musi posiadać narzędzie do przechowywania oraz zabezpieczania haseł i danych osobowych zdefiniowanych przez użytkownika.
2. Narzędzie to musi być dostępne na systemach Windows, macOS, Andorid oraz iOS.
3. Narzędzie to musi integrować się z przeglądarkami Microsoft Edge, Mozilla Firefox, Google Chrome.
4. Narzędzie musi posiadać funkcjonalność generowania nowych haseł, posiadających do 32 znaków.
5. Narzędzie musi posiadać funkcjonalność raportowania, która poinformuje m. in. o tym czy hasła jest słabe.
6. Narzędzie musi posiadać funkcjonalność zdalnego wylogowania z kont.

**Szyfrowanie danych**

1. Produkt musi posiadać funkcjonalność szyfrowania danych znajdujących się na dyskach wewnętrznych oraz wymiennych
2. Szyfrowanie danych musi odbywać się z wykorzystaniem algorytmu AES 256.
3. Zaszyfrowane dane na nośnikach wymiennych muszą być zdatne do odczytu na urządzeniu bez konieczności posiadania produktu zabezpieczającego.
4. **Oprogramowanie antywirusowe**

Oprogramowanie antywirusowe - okres ochrony: 2 lata, minimum 8 stanowisk.

**Administracja zdalna w chmurze**

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
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.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
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.
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.

**Ochrona stacji roboczych**

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
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.
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).
11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
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.
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.
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.
15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

* tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
* tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
* tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
* 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,
* tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

1. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
2. 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.
3. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
4. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
5. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

**Ochrona serwera**

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.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
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.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. 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.
6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.*
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
4. 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 zawieszonego mikro-serwisu.

**Ochrona urządzeń mobilnych opartych o system Android**

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:

a. usunięcie zawartości urządzenia,

b. przywrócenie urządzenie do ustawień fabrycznych,

c. zablokowania urządzenia,

d. uruchomienie sygnału dźwiękowego,

e. lokalizację GPS.

1. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
2. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
3. nazwę aplikacji,
4. nazwę pakietu,
5. kategorię sklepu Google Play,
6. uprawnienia aplikacji,
7. pochodzenie aplikacji z nieznanego źródła.

1. **Oprogramowanie antywirusowe – 2 sztuki**

Oprogramowanie antywirusowe - okres ochrony: 2 lata, minimum 5 stanowisk.

**Ochrona stacji roboczych - Windows**

1. Pełne wsparcie dla systemu Windows 10/Windows 11.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
4. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
5. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim oraz angielskim.

**Ochrona antywirusowa i antyspyware**

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
7. System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
9. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
13. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
14. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
15. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
16. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
17. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
18. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
19. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
20. Wbudowany konektor dla programów MS Outlook.
21. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
22. 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).
23. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
24. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
25. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
26. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
27. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
28. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
29. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
30. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
31. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
32. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
33. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
34. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
35. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
36. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
37. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
38. Możliwość automatycznego wysyłania nowych do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
39. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
40. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
41. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
42. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
43. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
44. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
45. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
46. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
47. Program ma umożliwiać 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.
48. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
49. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
50. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
51. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
52. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
53. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
54. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

* tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
* tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
* tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
* tryb uczenia się, w którym program 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,
* tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

1. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
2. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
3. Aplikacja musi posiadać dedykowaną funkcję, wykorzystującą technologię procesorów Intel (TDT) w zakresie zwiększenia skuteczności wykrywania zagrożeń wymuszających okup.
4. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
5. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
6. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
7. Funkcja, generująca taki log, ma posiadać przynajmniej 3 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
8. Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
9. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
10. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
11. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
12. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
13. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
14. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
15. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
16. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
17. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli rodzicielskiej i kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
18. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
19. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
20. Możliwość podejrzenia informacji o licencji, która znajduje się w programie.
21. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
22. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
23. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
24. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
25. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.
26. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
27. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
28. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.*
29. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
30. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

**Ochrona przed spamem**

1. Ochrona antyspamowa dla programów pocztowych MS Outlook.
2. Program ma umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
3. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
4. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
5. Możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
6. Możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
7. Możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
8. Program ma domyślnie współpracować z folderem „Wiadomości-śmieci”, dostępnym w programie Microsoft Outlook.
9. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana”
10. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana”.
11. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

**Zapora osobista (personal firewall)**

1. Zapora osobista ma pracować w jednym z czterech trybów:

* tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
* tryb interaktywny – program pyta się o każde nowo nawiązywane połączenie,
* tryb oparty na regułach – program blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
* tryb uczenia się – program automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

1. Program musi oceniać reguły zapory systemu Windows. 105. Możliwość tworzenia list sieci zaufanych.
2. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
3. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
4. Możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
5. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
6. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
7. Wykrywanie modyfikacji w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
8. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
9. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
10. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
11. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
12. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
13. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
14. Program musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów: z aplikacją lokalną, którą administrator wskazuje z listy, z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP.

**Kontrola rodzicielska**

1. Aplikacja musi być wyposażona w zintegrowany moduł kontroli rodzicielskiej.
2. Moduł Kontroli rodzicielskiej musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane reguły filtrowania.
3. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
4. Dla kont użytkowników musi istnieć możliwość przypisania gotowych profili filtrowania kategorii.
5. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
6. Podstawowe kategorie, w jakie aplikacja musi być co najmniej wyposażona to: Osoby dorosłe, Agresywne, Alkohol i wyroby tytoniowe, Ukrywające tożsamość, Sztuka, Motoryzacja, Biznes i praca, Czaty i sieci społecznościowe, komunikacja, Działalność przestępcza, Oświata, Rodzina i wychowanie dzieci, Moda, Finanse, Żywność i napoje, Zdrowie, Hobby i zainteresowania, Dzieci, Styl życia, Aktualności, Zwierzęta domowe, Zagadnienia społeczne, polityczne i prawne, Nieruchomości, Religia, Nauka, Edukacja seksualna, Zakupy, Sport, Technologie, Podróże
7. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta.
8. Dla poszczególnych kont użytkownik ma posiadać możliwość utworzenia wyjątków dla konkretnych adresów url, które mogą być wyświetlone nawet w przypadku, gdy dany adres znajduje się w którejkolwiek z blokowanych kategorii.
9. Aplikacja musi być wyposażona w moduł logowania zablokowanych stron oraz kategorii niezależnie od zalogowanego użytkownika.
10. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli rodzicielskiej.

**Ochrona Bankowości elektronicznej**

1. Aplikacja musi być wyposażona w moduł ochrony bankowości internetowej.
2. Przeglądarka powinna automatycznie szyfrować wszelkie dane wpisywane przez Użytkownika w formularzach internetowych. Szyfrowanie powinno odbywać się na poziomie odczytu znaków wpisywanych z klawiatury.
3. Użytkownik w każdym czasie musi mieć możliwość ręcznego uruchomienia przeglądarki w trybie zabezpieczonym modułem ochrony bankowości elektronicznej dla dowolnego adresu URL.
4. Praca w trybie bezpiecznym musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na pasku przeglądarki.

**Monitor sieci domowej**

1. Aplikacja ma posiadać moduł skanujący sieć domową, do której podłączony jest użytkownik, wyświetlając obecnie podłączone urządzenia sieciowe oraz sygnalizować nowo podłączane.
2. Wyświetlane hosty widoczne są pod ich nazwą NETBIOS, adresem IP oraz adresem MAC. Wraz z tymi informacjami wyświetlane muszą być informacje na temat ostatniego wykrycia hosta.
3. Wyświetlana nazwa hosta może być modyfikowana przez użytkownika.
4. Aplikacja musi być wyposażona w mechanizm umożliwiający tworzenie reguł dla ostatnio zablokowanej komunikacji, użytkownik musi mieć możliwość wyświetlania komunikacji, jaka była blokowana w ostatnim czasie (co najmniej ostanie 5,15,60 minut).
5. Użytkownik ma możliwość otwarcia interfejsu logowania się do swojego urządzenia brzegowego (routera itp.) poprzez link umieszczony w menu aplikacji.
6. Moduł ochrony sieci musi mieć możliwość przeprowadzenia audytu zabezpieczeń routera znajdującego się w sieci użytkownika.
7. System skanowania routera musi mieć możliwość wykrycia co najmniej otwartych portów sieciowych, zabezpieczenia konfiguracji urządzenia za pomocą domyślnych lub słabych haseł.
8. Moduł ochrony sieci domowej wykonujący skanowanie pod kątem otwartych portów powinien sprawdzać co najmniej porty 80, 443, 139, 445, 21, 22, 23.
9. Moduł musi wykrywać również urządzenia podłączone w sieci domowej należące do grupy produktów „Internet of Things”.
10. Moduł ten musi mieć możliwość wykrycia, czy urządzenie pracuje w sieci publicznej czy lokalnej. W przypadku sieci publicznej program musi wyświetlić ostrzeżenie użytkownikowi o ryzyku skanowania w takim trybie.

**Ochrona kamery internetowej**

1. Aplikacja ma umożliwiać kontrolę użycia kamery internetowej przez procesy znajdujące się w systemie jak i inne aplikacje.
2. W przypadku próby użycia kamery przez aplikację lub proces systemowy, użytkownikowi musi wyświetlić się stosowny komunikat ostrzegawczy.
3. Wykrycie próby użycia kamery musi dać użytkownikowi możliwość zezwolenia lub blokady takiej czynności.
4. Użytkownik może utworzyć listę aplikacji, które będą miały dostęp do kamery. Analogiczna lista musi zostać utworzona dla aplikacji, dla których wykonywana będzie blokada.

**Ochrona antykradzieżowa**

1. Program musi posiadać moduł umożliwiający powiązanie zainstalowanego w systemie pakietu ochrony z kontem utworzonym na dedykowanym serwisie online dostępnym za pomocą przeglądarki internetowej na serwerach producenta.
2. Po zalogowaniu do swojego indywidualnego konta na portalu producenta użytkownik powinien mieć wylistowane urządzenia, z którymi jest to konto powiązane.
3. Logowanie do portalu za pomocą przeglądarki internetowej musi odbywać się poprzez zabezpieczoną komunikację HTTPS.
4. Portal musi posiadać polski interfejs.
5. Użytkownik z poziomu swojego konta musi posiadać możliwość wykonania testu na widocznym w portalu swoim komputerze w celu weryfikacji poprawności działania modułu antykradzieżowego.
6. Wyzwolenie zadania testu musi wymagać potwierdzenia jego wykonania od strony użytkownika urządzenia, na którym test ma być wykonany.
7. W trakcie testu mechanizmy wbudowane w pakiet antywirusowy muszą zebrać co najmniej informację o: lokalizacji testowanego komputera ( jeśli jest ona dostępna ) – urządzenie powinno być wskazane na mapie w postaci graficznej, wykonać screenshoot’a pulpitu oraz wykonać zdjęcie za pomocą wbudowanej w komputer kamery (jeśli jest dostępna) i zebrać informację o adresie IP, z jakiego łączy się testowany komputer.
8. Zebrane podczas testów informacje muszą być widoczne dla zalogowanego na portalu użytkownika.
9. W przypadku kradzieży lub zagubienia urządzenia, Użytkownik musi posiadać możliwość określenia swojego urządzenia jako brakującego.
10. W momencie, gdy urządzenie zostanie określone jako brakujące, automatycznie musi zostać przesłane na nie zadanie aktywacji dedykowanego konta systemowego z ograniczeniami, oraz wymuszenie restartu systemu Windows.
11. Po restarcie komputera musi istnieć możliwość zalogowania się jedynie do konta z ograniczeniami utworzonego przez mechanizmy auto ochrony, pozostałe konta systemowe mają być nieaktywne.
12. Mechanizm antykradzieżowy w momencie aktywacji ma automatycznie tworzyć zdjęcia przy wykorzystaniu wbudowanej w urządzenie kamery (jeśli dostępna), zapisywać obraz pulpitu, zbierać informacje odnośnie lokalizacji urządzenia oraz wykorzystywanych adresów IP.
13. Zebrane informacje mają zostać przesłane na konto użytkownika utworzone na portalu producenta.
14. W przypadku braku połączenia z siecią Internet, w/w informacje maja być zbierane i przesłane do portalu w momencie, gdy urządzenie będzie posiadało aktywne połączenie z siecią Internet.
15. Zalogowany do konta na portalu producenta użytkownik musi posiadać możliwość zdalnego wyświetlenia na brakującym urządzeniu dowolnego komunikatu zawierającego tekst i obraz.
16. Z poziomu portalu, użytkownik musi mieć dostęp do danych historycznych wcześniej zebranych podczas testów lub w momencie określenia urządzenia jako brakującego.
17. Użytkownik musi posiadać opcję usunięcia swojego konta z serwerów producenta wraz z informacjami tam się znajdującymi.

**Menedżer licencji**

1. Interfejs menedżera licencji musi być dostępny z poziomu strony WWW.
2. Dostęp do witryny musi być zabezpieczony z pomocą SSL.
3. Interfejs webowy musi być dostępny w języku polskim.
4. Interfejs www musi posiadać możliwość dodania więcej niż jednej licencji.
5. Produkt zabezpieczający musi posiadać możliwość aktywacji przy pomocy danych logowania menedżera licencji.
6. Komputer po aktywacji musi się zgłaszać do menedżera licencji za pomocą nazwy NETBIOS.
7. Menedżer musi pokazywać liczbę wykorzystanych i dostępnych licencji.
8. Musi być możliwość zmiany nazwy komputera na stornie www po dokonaniu aktywacji .
9. Dezaktywacja licencji musi być dostępna bezpośrednio z interfejsu www.
10. Przy usuwaniu licencji z interfejsu www musi być dostępna opcja dezaktywacji wszystkich stacji.

**Prywatność i zabezpieczenia przeglądarki**

1. Czyszczenie danych przeglądarki musi być obsługiwane przez rozszerzenie instalowane bezpośrednio w przeglądarkach Google Chrome, Mozilla Firefox oraz Microsoft Edge.
2. Produkt musi pozwalać na usuwanie danych przeglądarki, minimum: historia pobierania, historia przeglądania, pliki cookie, obrazy i pliki zapisane w pamięci podręcznej, hasła i dane logowania, autouzupełnianie danych formularzy.
3. Produkt musi zezwalać na tworzenie listy stron internetowych, których czyszczenie danych przeglądarki nie dotyczy.
4. Produkt musi pozwalać na czyszczenie w trybie jednorazowym bądź cyklicznym.
5. Produkt musi posiadać funkcjonalność skanującą wyniki wyszukiwania i wyświetlać informacje o tym czy witryna jest bezpieczna.

**Sandbox w chmurze**

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
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.
4. Użytkownik musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Użytkownik musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Użytkownik musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
8. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej.

W przypadku wykrycia zagrożenia, komputer jest bezzwłocznie chroniony.

1. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

**Menadżer haseł**

1. Produkt musi posiadać narzędzie do przechowywania oraz zabezpieczania haseł i danych osobowych zdefiniowanych przez użytkownika.
2. Narzędzie to musi być dostępne na systemach Windows, macOS, Andorid oraz iOS.
3. Narzędzie to musi integrować się z przeglądarkami Microsoft Edge, Mozilla Firefox, Google Chrome.
4. Narzędzie musi posiadać funkcjonalność generowania nowych haseł, posiadających do 32 znaków.
5. Narzędzie musi posiadać funkcjonalność raportowania, która poinformuje m. in. o tym czy hasła jest słabe.
6. Narzędzie musi posiadać funkcjonalność zdalnego wylogowania z kont.

**Szyfrowanie danych**

1. Produkt musi posiadać funkcjonalność szyfrowania danych znajdujących się na dyskach wewnętrznych oraz wymiennych
2. Szyfrowanie danych musi odbywać się z wykorzystaniem algorytmu AES 256.
3. Zaszyfrowane dane na nośnikach wymiennych muszą być zdatne do odczytu na urządzeniu bez konieczności posiadania produktu zabezpieczającego.
4. **Oprogramowanie przeciwdziałające wyciekowi danych – 77 sztuk**

Licencja wieczysta z 2 letnim okresem wsparcia dla 77 stanowisk.

Oprogramowanie przeciwdziałające wyciekowi danych w łącznej ilości 77 sztuk rozdzielonej na osobne paczki zarządzane oddzielnie w ilościach:

* 7 sztuk,
* 15 sztuk,
* 55 sztuk,

Minimalne wymagania Zamawiającego

**Ochrona przed wyciekiem danych**

1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows 11 z najnowszymi aktualizacjami.
2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych.
3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim.
4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL.
6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
8. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.
9. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.
11. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania: kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.
12. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.
13. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania.
14. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania oraz klonowania.
15. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:

* Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
* Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.

1. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory.
2. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:
3. logowanie oraz wylogowanie użytkownika,
4. włączenie oraz wyłączenie stacji roboczej,
5. blokada oraz odblokowanie stacji roboczej,
6. przejście w stan bezczynności stacji roboczej.
7. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie zbliżonym do rzeczywistego.
8. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.
9. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.
10. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF bądź XLS.
11. Serwer musi posiadać możliwość wysłania alertów co najmniej za pośrednictwem wiadomości email oraz za pomocą SIEM/SYSLOG.
12. Serwer administracyjny musi posiadać możliwość konfiguracji cyklicznych raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
13. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
14. Raporty muszą być generowane do pliku PDF i/lub XLS, zapisywane w lokalizacji na serwerze lub na wskazany adres(y) e-mail.
15. Serwer administracyjny musi posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania, ale również umożliwiać jego zmianę na serwer klienta.
16. Serwer administracyjny musi posiadać możliwość wyszukiwania plików w oparciu o ich zawartość, co najmniej o:

a) numery kart kredytowych,

b) numer PESEL,

c) numer polskiego dowodu osobistego,

d) polski numer paszportu,

e) wyrażenia regularne,

f) określone ciągi znaków,

g) numer IBAN.

1. Weryfikacja zawartości pliku powinna odbywać się w czasie rzeczywistym.
2. System musi posiadać możliwość importu własnych słowników do klasyfikowania danych.
3. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych od jakich plik zostanie sklasyfikowany.
4. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na:

a) audyt i logowanie wiadomości e-mail,

b) audyt i logowanie operacji na plikach.

1. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi.
2. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu które są podzielone na:

a) Bezpieczeństwo danych:

• Przegląd informacji o incydentach bezpieczeństwa.

• Przegląd danych przychodzących.

• Przegląd danych wychodzących.

• Przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików.

• Podłączane/odłączane urządzenia przenośne.

b) Produktywność:

• Przegląd informacji na temat produktywności użytkowników.

• Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.

c) Eksploatacja sprzętu:

• Przegląd informacji na temat eksploatacji sprzętu komputerowego.

• Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.

• Eksploatacja drukarek.

• Eksploatacji sieci.

1. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.
2. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
3. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt:

• plików przenoszonych na nośniki USB i inne urządzenia przenośne,

• plików przesłanych za pomocą wiadomości e-mail,

• plików przesłanych za pomocą poczty webowej,

• plików przesłanych do Internetu,

• plików wysłanych za pomocą komunikatorów,

• plików przesłanych na dyski chmurowe,

• analiza sposobu korzystania z aplikacji,

• analiza korzystania z Internetu,

• analiza wykorzystania portali do poszukiwania pracy

1. **Wdrożenie systemów teleinformatycznych**

Usługi wdrożeniowe oprogramowania przeciwdziałającego wyciekowi danych (DLP), którego głównym celem jest zabezpieczenie przed utratą lub nieautoryzowanym dostępem do informacji poufnych. Oprogramowanie to ma zostać zainstalowane na serwerze działającym pod kontrolą systemu Windows Server co najmniej w wersji 2016 oraz powinno być obsługiwane za pomocą dwóch konsol: aplikacyjnej i webowej, w celu ułatwienia zarządzania systemem.

1. Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.
2. Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.
3. Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.
4. Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.
5. Wykonawca zainstaluje oprogramowanie przeciwdziałającego wyciekowi danych.
6. Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.
7. Wykonawca uruchomieni i skonfiguruje konsolę zarządzającą, wprowadzi klucz dostępowy i usunie dane demonstracyjne.
8. Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.
9. Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze oraz urządzeniach końcowych.
10. Wykonawca wykona konfigurację kategorii danych i danych wrażliwych oraz zdefiniuje wykrywanie kategorii:

* Numery kart kredytowych
* Numery IBAN
* Numery dowodów osobistych
* Polski numer paszportu
* Numer PESEL

1. Wykonawca skonfiguruje alerty związane z usługami oraz zabezpieczeniem DLP oraz przetestuje poprawność ich działania na danych testowych.
2. Wykonawca skonfiguruje zadania archiwizacji danych oraz usuwania starych wpisów z bazy danych.
3. Wykonawca przetestuje działanie polityk i wprowadzi ich aktualizację w przypadku wykrycia braku ich skutecznego działania.
4. Wykonawca wygeneruje z prawidłowo wdrożonego oprogramowania raport audytu bezpieczeństwa i przeprowadzi analizę aktywności użytkowników oraz przepływu informacji w organizacji.
5. Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje.
6. Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.
7. Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii.

**Część 9 Dostawa oprogramowania do monitorowania infrastruktury.**

1. **Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej w łącznej ilości 195 sztuk.**

Oprogramowanie do zarzadzania i aktualizacji w łącznej ilości 195 sztuk rozdzielonej na osobne paczki zarządzane oddzielnie w ilościach:

* 70 sztuk,
* 20 sztuk,
* 20 sztuk,
* 35 sztuk,
* 35 sztuk,
* 15 sztuk.

Oprogramowanie musi spełniać następujące wymagania w zakresie zarządzania zasobami IT:

* Zarządza wszystkimi zasobami, za które odpowiada dział IT.
* Pokazuje szczegółowe informacje i ewidencję czynności wykonanych na zasobach w trakcie całego cyklu życia.
* Ma możliwość definiowania statusów i pól oraz generowanie protokołu przekazania sprzętu.
* Potrafi przypisać dokument do wielu zasobów.
* Generuje dokumenty na podstawie szablonów.
* Automatycznie numeruje dodawane zasoby i dokumenty według zdefiniowanego wzorca numeracji.
* Posiada system zarządzania aplikacjami i licencjami.
* System identyfikuje realne zużycie licencji.
* Rozlicza licencje według użytkownika, urządzenia, numeru seryjnego lub na podstawie wersji zainstalowanej aplikacji.
* Posiada historię użycia konkretnych licencji oprogramowania.
* Oprogramowanie robi audyt inwentaryzacji sprzętu i oprogramowania.
* Posiada zdalny dostęp do managera plików z możliwością usuwania plików użytkownika.
* System zbiera informacje o wpisach rejestrowych, plikach, archiwach oraz konfiguracji sprzętowej konkretnych stacji roboczych.
* Zarządza instalacjami/dezinstalacjami oprogramowania w oparciu o menadżera pakietów MSI.
* Ma możliwość archiwizacji i porównywania audytów.
* Monitoruje harmonogram zadań Windows.

Oprogramowanie musi spełniać następujące wymagania w zakresie zarządzania użytkownikami:

* Zarządza użytkownikami, bazując na grupach i politykach bezpieczeństwa.
* Przyporządkowuje dane do konkretnego użytkownika.
* Blokuje niebezpieczne domeny WWW.
* Chroni pracowników przed wiadomościami phishingowymi i atakami APT.
* Rozróżnia wykonywane czynności na poszczególnych urządzeniach.
* Posiada rejestr naruszeń blokad, który agreguje informacje o próbach dostępu do blokowanych stron.
* Posiada dedykowane alarmy dla wszystkich rodzajów incydentów zbieranych przez rejestr naruszeń blokad.
* Ma możliwość blokowania uruchamianych aplikacji.
* Może korzystać z zewnętrznych list blokowania stron takich jak listę ostrzeżeń CERT.PL
* Monitoruje wiadomości e-mail.
* Zbiera informacje o odwiedzanych stronach WWW.
* Monitoruje użycie łącza przez poszczególnych użytkowników.
* Zarządza regułami blokowania aplikacji i stron WWW.
* Ma możliwość wykrywania podejrzanych aktywności użytkowników za pomocą mechanizmu wykrywania jigglerów.

Oprogramowanie musi spełniać następujące wymagania w zakresie pomocy technicznej:

* Posiada tworzenie zgłoszeń serwisowych i zarządza nimi.
* Ma możliwość wskazania osób, które muszą zaakceptować zgłoszenie.
* Tworzy ścieżki akceptacji na podstawie kategorii przypisanej do zgłoszenia.
* Posiada możliwość stworzenia listy aplikacji bezpiecznych do samodzielnej instalacji przez użytkownika.
* Może przetwarzać zgłoszenia w trybie anonimowym.
* Posiada rozbudowany system raportów.
* Ma bazę zgłoszeń z rozbudowaną wyszukiwarką.
* Posiada wewnętrzny komunikator z możliwością przesyłania plików oraz przydzielania uprawnień.
* Oprogramowanie posiada zdalny dostęp do komputerów z możliwością blokowania myszy/klawiatury.
* Ma równoczesny zdalny dostęp kilku administratorów do jednego agenta.
* Posiada integrację bazy użytkowników z Active Directory.
* Zarządza kontami lokalnych użytkowników Windows.

Oprogramowanie musi spełniać następujące wymagania w zakresie kontroli dostępu do danych:

* Automatycznie nadaje użytkownikom domyślną politykę monitorowania i bezpieczeństwa.
* Monitoruje operacje na plikach z zasobów sieciowych udostępnianych przez urządzenia.
* Zabezpiecza sieć przed wirusami instalującymi się automatycznie z pendrive’ów lub dysków zewnętrznych.
* Posiada integrację z Windows Defender, Windows Firewall i Windows Bitlocker.
* Alarmy o podłączonym urządzeniu obcym.
* Możliwość zdalnego szyfrowania dysków.
* Zbiera informacje o urządzeniach podłączonych do danego komputera.
* Posiada bazę wszystkich urządzeń podłączonych do komputerów w sieci.
* Posiada historię połączeń i operacji na urządzeniach przenośnych.
* Zarządza prawami dostępu.
* Ustawia reguły dla całej sieci.

Oprogramowanie musi spełniać następujące wymagania w zakresie zarządzania czasem:

* Posiada statystyki czasu spędzonego przed komputerem.
* Ma możliwość tworzenia grup złożonych z dowolnych pracowników w firmie.
* Posiada listę aplikacji używanych przez poszczególnych pracowników .
* Dodawanie dostępu do odpowiednich aplikacji dla danych grup pracowników.
* Możliwość oznaczania stron internetowych i aplikacji jako produktywne, neutralne lub nieproduktywne.
* Posiada listę kontaktów w danej organizacji.
* Podgląd zrzutu ekrany wybranego użytkownika dostępny dla menadżerów i administratorów.

1. **Platforma szkoleniowa – 55 użytkowników**

Minimalne wymagania zamawiającego:

* Platforma posiada materiały szkoleniowe od ekspertów z cyberbezpieczeństwa;
* Zawiera testy i praktyczne zadania utrwalające wiedzę;
* Monitoruje postępy, statystyki pracowników i zespołów;
* Posiada aktualne informacje o najnowszych zagrożeniach i sposobach ataków;
* Zawiera comiesięczne newslettery edukacyjne;
* Ma możliwość powrotu do lekcji w dowolnym momencie;
* Platforma posiada zarządzanie grupami i użytkownikami;
* Posiada statystyki wskazujące osoby i zespoły najbardziej podatne na ataki;
* Ma możliwość wglądu przez menadżerów i adminów w cały proces nauki pracowników;
* Posiada raporty prezentujące osiągnięcia działów i zespołów;
* Ma co najmniej 65 lekcji z zakresu cyberbezpieczeństwa;
* Posiada co najmniej 12 modułów podzielonych tematycznie;
* Ma co najmniej 17 testów sprawdzających wiedzę.

W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych Wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia   
w wystarczająco precyzyjny i zrozumiały sposób i jest to uzasadnione specyfiką przedmiotu zamówienia.   
W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”. W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, ocen technicznych, specyfikacji technicznych   
i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 Pzp, **Zamawiający dopuszcza rozwiązania równoważne opisywanym,** **a wskazane powyżej odniesienia należy odczytywać   
z wyrazami „lub równoważne”.** Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i funkcjonalne spełniające co najmniej warunki określone w opisie przedmiotu zamówienia. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany udowodnić w ofercie, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w szczegółowym opisie przedmiotu zamówienia.