Załącznik nr A do SWZ Opis przedmiotu zamówienia

ZNAK SPRAWY: RZP-II.271.26.2022

**Część I: Sprzęt komputerowy i oprogramowanie biurowe**

|  |
| --- |
| **Zakup zestawów komputerowych stacjonarnych – 6 szt.** Zestawy komputerowe stacjonarne z monitorem i UPS’em.  |
| Płyta główna: | zaprojektowana przez producenta komputera |
| Procesor: | min. 6-rdzeniowy, min. 12425 punktów w teście PassMark - CPU Mark dla konfiguracji jednoprocesorowej. Minimum 12MB pamięci podręcznejMinimum 12T wątkówMinimum 3.2GHz – 4.6GHz. |
| Chipset: | TPM |
| Pamięć RAM: | Min. 16 GB SDRAM DDR4  |
| Karta graficzna: | min. zintegrowana z płytą główną  |
| Wbudowane porty: | 1. Minimum 4 porty USB,
2. Minimum 1 złącze HDMI
3. Minimum 1 port RJ45,
4. Złącze lub złącza audio,
 |
| Interfejsy sieciowe: | Min. 1Gb Ethernet w standardzie Base-T;  |
| Pamięć masowa: | Dysk SSD Min. 512 GB  |
| Zasilanie: | zasilacz 220V |
| Napęd dysków optycznych: | DVD±RW SATA |
| Wyposażenie multimedialne: | Min. zintegrowana, zgodna z High Definition (HD) Audio, mikrofon i głośnik  |
| Urządzenie sterujące: | 1. Klawiatura w układzie QWERTY z wydzieloną częścią numeryczną, minimum 104 klawisze
2. Mysz optyczna z dwoma klawiszami oraz rolką (scroll) zgodna z portami płyty głównej,
 |
| BIOS: | BIOS w oferowanym komputerze powinien posiadać funkcjonalność:1. Bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:
2. wersji BIOS’u, oraz dacie jego powstania,
3. nazwie produktu,
4. numerze seryjnym,
5. typie procesora, wraz z informacją o jego taktowaniu, ilości rdzeni i ID, wielkości pamięci cache,
6. wielkości zainstalowanej pamięci RAM, magistrali na jakiej pracuje oraz o jej typie.
7. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń,
8. Możliwość ustawienia hasła
 |
| Gwarancja: | 1. Min. 3-letnia gwarancja sprzętu door-to-door
2. Możliwość sprawdzenia statusu gwarancji online, pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji.
 |
| Certyfikaty: | Zgodny z normą ISO-9001, deklaracja CE |
| Oprogramowanie systemowe: | Windows 10 Professional 64-bit lub Microsoft Windows 11 Professional 64-bit w wersji OEM w polskiej wersji językowej pre-instalowany z ukrytej przestrzeni dysku,  |
| Wymagania dodatkowe: | Zamawiający nie dopuszcza stosowania plomb blokujących możliwość rozbudowy komputera których zerwanie może powodować utratę lub pogorszenie warunków gwarancji, |
| Monitor | Typ ekranu IPS, o przekątnej min. 23,8” o rozdzielczości min. 1920x1080 pikseli. Jeżeli nie ma głośników zew. lub wbudowanych w komputer muszą być głośniki wbudowane w monitor. W monitorze powinno być co najmniej gniazdo i kabel połączeniowy typu HDMI Mini. 2-letni serwis monitora w trybie „door to door”.  |
| UPS | Zasilacz UPS do podtrzymywania napięcia na wypadek braku prądu. W komplecie muszą być kable pozwalające podłączyć stację roboczą i monitor. Oprogramowanie do komputera współpracujące z UPS’em – informujące użytkownika o braku zasilania. Minimum 800VA/300W. |

|  |
| --- |
| **Komputery przenośne – 5 szt.**Komputery do zdalnego dostępu i pracy zdalnej. |
| Przekątna ekranu | Minimum 15,6”  |
| Matryca | min. 1980 x 1080, IPS, Anti-glare |
| Płyta główna: | Zaprojektowana przez producenta komputera |
| Procesor: | Minimum 4-rdzeniowy, min. 6384 punktów w teście PassMark - CPU Mark. Minimum 8 MB cache, Minimum 1.1GHz, Buss Speed 4GT/s |
| Chipset: | TPM |
| Pamięć RAM: | Min. 16 GB DDR4 |
| Karta graficzna: | Zintegrowana |
| Wbudowane porty i media: | 1. Minimum 2 porty USB typu C
2. Minimum 1 złącze HDMI
3. Minimum 1 port RJ45,
4. Czytnik kart pamięci microSD,
5. Min. 1 uniwersalne gniazdo słuchawkowe/mikrofonowe.
6. złącze Kensington
 |
| Interfejsy sieciowe: | 1. Min. jeden Interfejs sieciowy 1Gb Ethernet w standardzie Base-T
2. Jeden interfejs sieci bezprzewodowej WiFi
3. Interfejs Bluetooth
 |
| Pamięć masowa: | dysk SSD Min. 256 GB  |
| Zasilanie: | Akumulator, 4-ogniwowa bateria 63 Wh z obsługą funkcji ExpressCharge Zasilacz prądu przemiennego 230V ze złączem USB Type-C, przewód min. 1m |
| Wyposażenie multimedialne: | Karta dźwiękowa zintegrowana, zgodna z High Definition (HD) Audio, HD + IR kamera z mikrofonem |
| Urządzenie sterujące: | 1. Klawiatura w układzie QWERTY, z blokiem numerycznym,
2. Touch Pad (płytka dotykowa) zawierająca:
3. Minimum dwa przyciski wyboru
4. Funkcję przewijania (góra/dół, prawo/lewo)
5. Dodatkowa bezprzewodowa mysz optyczna, 2 przyciski + rolka
 |
| BIOS: | BIOS w oferowanym komputerze powinien posiadać funkcjonalność:1. Bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:
2. wersji BIOS’u, oraz dacie jego powstania,
3. nazwie produktu,
4. numerze seryjnym,
5. typie procesora, wraz z informacją o jego taktowaniu, ilości rdzeni i ID, wielkości pamięci cache,
6. wielkości zainstalowanej pamięci RAM, magistrali na jakiej pracuje oraz o jej typie.
7. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń,
8. Możliwość ustawienia hasła
9. Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej oraz kontrolera USB z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
 |
| Gwarancja: | 1. Min. 3 letnia gwarancja producenta typu „Door to door”
2. Możliwość sprawdzenia statusu gwarancji, pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji.
 |
| Oprogramowanie systemowe: | Windows 10 Professional 64-bit lub Microsoft Windows 11 Professional 64-bit w wersji OEM w polskiej wersji językowej pre-instalowany z ukrytej przestrzeni dysku,  |
| Wymagania dodatkowe: | Zamawiający nie dopuszcza stosowania plomb blokujących możliwość rozbudowy komputera których zerwanie może powodować utratę lub pogorszenie warunków gwarancji, |

|  |
| --- |
| **Pakiet biurowy - oprogramowanie – 11 szt.**Zamawiający opisując pakiet oprogramowania biurowego ma szczególnie na uwadze, aby dokumenty, które są tworzone przy użyciu tego pakietu mogły być współdzielone bez utraty formatowania z innymi już używanymi pakietami przez Zamawiającego tj. MS Office 2013, MS Office 2016 i MS Office 2019. Oprogramowanie musi być w pełni kompatybilne w zakresie użytkowym i funkcjonalnym z już używanymi przez Zamawiającego pakietami MS Office. |
| 1. Polska wersja językowa,
2. Najnowsza wersja udostępniana przez producenta,
3. Oprogramowanie musi być kompatybilne w zakresie funkcjonalności, formatowania, sposób zapisu danych z innymi używanymi przez Zamawiającego pakietami MS Office,
4. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy),
5. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim,
6. Wymaga się dostarczenia oprogramowania na nośniku danych lub poprzez udostępnienie możliwości pobrania oprogramowania ze strony producenta na podstawie dostarczonej licencji,
7. Wymagane jest wsparcie producenta.
 |

|  |
| --- |
| **Serwer – 1 szt.**Serwer ma umożliwić prawidłowe zarządzanie i monitorowanie systemów zabezpieczeń sieci. Serwer będzie służył do utrzymania w zwirtualizowanym środowisku usług zarządzania i monitorowania systemów zabezpieczeń sieci Zamawiającego. Podana wydajność serwera pozwoli sprostać wymaganiom systemu rejestrowania, korelacji oraz raportowania i zarządzania incydentami. |
| Obudowa: | Obudowa typu Rack wraz z miejscem na minimum 4 dyski, komplet szyn z organizatorem okablowania umożliwiającym montaż w standardowej szafie Rack |
| Płyta główna: | Płyta główna musi być zaprojektowana przez producenta serwera  |
| Procesor: | Co najmniej jeden procesor z co najmniej:* 8 rdzeni/16 wątków/16 MB cache
* Minimalna prędkość UPI 8GT/s
 |
| Chipset: | Dedykowany przez producenta procesora  |
| Pamięć RAM: | Minimum 64 GB pamięci RAM  |
| Karta graficzna: | min. Zintegrowana karta graficzna  |
| Wbudowane porty: | 1. Minimum 1 port USB 3.0 z przodu oraz 2 porty z tyłu,
2. Minimum 1 port VGA
 |
| Interfejsy sieciowe: | 1. Minimum dwa wbudowane interfejsy sieciowe 1Gb Ethernet w standardzie Base-T,
 |
| Kontroler dysków: | Sprzętowy kontroler dyskowy umożliwiający skonfigurowanie na wewnętrznej pamięci dyskowej zabezpieczeń RAID: 0, 1, 5, 10 |
| Pamięć masowa: | Zamawiający dopuszcza następujące konfiguracje:1. Zainstalowane minimum 2 dyski o minimalnej pojemności 960GB SSD SATA Read Intensive (RAID 1) Hot Plug
2. Zainstalowane minimum 2 dyski o minimalnej pojemności 2,4TB, SAS 12Gb/s 10 tys. obr./min. (RAID 1)

lub1. Zainstalowane minimum 4 dyski o minimalnej pojemności 2,4TB, SAS 12Gb/s 10 tys. obr./min. (RAID 5)
2. Dyski SSD powinny być skonfigurowane w RAID 1 dla systemu operacyjnego i aplikacji
3. Dyski SAS powinny być skonfigurowane w RAID 1 na dane.
4. Napęd DVD (w przypadku braku wbudowanego napędu DVD dopuszcza się napęd zewnętrzny podłączany za pomocą USB)
 |
| Bezpieczeństwo i diagnostyka: | Fabryczne oznaczenie urządzenia, wykonane przez producenta serwera informujące zamawiającego m.in. o numerze serwisowym serwera, modelu serwera; |
| Gwarancja: | 1. Minimum trzy lata gwarancji door-to-door,
2. Możliwość zgłaszania awarii on-line
3. Możliwość sprawdzenia statusu gwarancji online poprzez wprowadzenie unikatowego numeru urządzenia na stronie producenta, pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera,
 |
| Wymagania dodatkowe: | 1. Zamawiający nie dopuszcza stosowania plomb blokujących możliwość rozbudowy komputera których zerwanie może powodować utratę lub pogorszenie warunków gwarancji,
 |
| System operacyjny serwera: | 1. Minimum Microsoft Windows Server 2022 wraz z licencjami dostępowymi CAL dla 30 użytkowników,
2. W komplecie nośnik DVD z systemem operacyjnym.
 |

Ogólne wymagania dla oferowanego sprzętu i oprogramowania dla części 1

|  |  |
| --- | --- |
| Certyfikaty dla sprzętu: | Deklaracja zgodności CE (załączyć do oferty).Certyfikat Energy Efficiency Certification. |
| Uaktualnienia dla oferowanego sprzętu: | Dostęp do aktualizacji systemu BIOS, podręczników użytkownika, najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta komputera numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony. |
| Serwis | Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta na terenie Rzeczpospolitej Polskiej. |
| Wsparcie Oferenta | Do oferty należy dołączyć karty katalogowe/specyfikacje techniczną urządzeń. Karta powinna zawierać wyraźne zdjęcia obudowy oferowanego komputera, komputera przenośnego i serwera.  |
| Inne | Wszystkie urządzenia muszą być fabrycznie nowe i dostarczone przez autoryzowany kanał sprzedaży producenta na terenie kraju.W komplecie nośnik DVD z systemem operacyjnym oraz z pakietem biurowym lub instrukcja w jaki sposób pobrać i zainstalować oprogramowanie. Lista kluczy oprogramowania przypisanego do określonego numeru seryjnego oferowanego urządzenia. |

**Część II: System do backupu:**

|  |
| --- |
| **Program do backup’u – komplet na 35 stacji i 2 serwery oraz 2 wirtualizatory HyperV**System do wykonywania kopii zapasowych kopii zapasowych na nową dostarczoną macierz w niniejszym postępowaniu. |
| Liczba komputerów objęta wykonywaniem kopii zapasowych | 35 |
| Liczba serwerów z systemem operacyjnym Linux i bazą postgree | 1 |
| Liczba serwerów z systemem MS Windows Server 2016/2022 | 1 |
| Liczba baz danych MS SQL Server | 2 |
| Liczba maszyn wirtualnych HyperV | 2 |
| Licencjonowanie: | **Licencje powinny pozwalać na zabezpieczenie:*** + **35 fizycznych stacji roboczych,**
	+ **2 fizycznych serwerów bez wirtualizacji,**
	+ **2 fizyczne hosty maszyn wirtualnych.**

Wsparcie techniczne:* Świadczone jest w języku polskim,
* Zapewnia dostęp do aktualizacji oprogramowania,
* Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego,
* Obowiązuje przez okres minimum 36 miesięcy.
* Dostęp do dokumentacji instalatora i użytkownika
* System po ustaniu wsparcia musi działać bezprzerwowo dalej z pełnymi możliwościami zarządzania przez administratora, jednakże Zamawiający zgadza się na odebranie prawa dostępu do aktualizacji i wsparcia
 |
| Centralne zarządzanie | TAK |
| Konfiguracja agentów | Agent może być zainstalowany na każdym sprzęcie z systemem Windows, Linux |
| Funkcjonalności | * Tworzenie kopii zapasowych obrazu dysku komputera wraz z systemem, aplikacjami i ustawieniami.
* Okno backupu, retencja, schematy rotacji, kompresja, szyfrowanie, rozłożenie startu
 |
| Ogólne informacje: | * Oprogramowanie może być dostarczane w co najmniej scenariuszu On-premise.
* Interfejs systemu dostępny jest w języku polskim,
* Oprogramowanie nie preferuje platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych,
* Możliwość instalacji oraz uruchomienia serwera zarządzania na maszynie wirtualnej opartych o systemy Windows Server: 2016 lub 2022
* System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji,
* Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju),
 |
| Wsparcie techniczne | * Pomoc techniczna w językach: polskim.
* Materiały samopomocowe: Baza wiedzy (polski)
 |
| Zarządzanie | * Zarządzanie całością działania systemu (backup, przywracanie) z poziomu jednej konsoli webowej,
* Zarządzanie całym systemem poprzez dashboardy,
* Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego,
* System posiada wbudowane predefiniowane zadania backupowe,
* System umożliwia tworzenie zadań backupowych w oparciu o kalendarz.
* Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem,
* Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem,
* Monitorowanie postępu działania zadania,
* Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach:
	+ Zadanie zostało zakończone pomyślnie,
	+ Zadanie zostało zakończone z ostrzeżeniami,
	+ Zadanie zostało zakończone z błędem,
	+ Zadanie zostało anulowane,
	+ Zadanie nie zostało uruchomione.
* System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego.
* Możliwość zdefiniowania okna backupowego dla każdego z zadań,
* Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów,
* System pozwala na klonowanie planów kopii zapasowych,
* System umożliwia reset hasła administratora w przypadku jego utraty,
* Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami,
* Oprogramowanie umożliwia tworzenie grup urządzeń,
* Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych,
* System pozwala na zarządzanie i umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami.
 |
| Składowanie danych | * System ma umożliwiać składowanie danych:
	+ Lokalnie: Zasób SMB, Zasób NFS,
	+ Opcjonalnie w chmurze dostarczanej przez producenta.
* System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji,
* System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
 |
| Odtwarzanie | * Odtwarzanie granularne:
	+ Pojedynczych plików z kopii obrazu dysku,
	+ Z kopii skrzynki pocztowej Microsoft 365,
* kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:
	+ Windows: 7, 10, 11
	+ Windows Server: 2008 R2,2016, 2022
* Odtwarzanie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
* Jedną z opcji odtwarzania ma odbywać się z bootowalnej płyty CD lub pendrive’a,
* Odtwarzanie zasobów plikowych z prawami dostępu,
* Przywracanie plików pomiędzy systemami operacyjnymi (np. odtwarzanie danych plikowych Linux na systemie Windows),
* Przywracanie danych z określonego urządzenia/użytkownika,
* Przywracanie kopii z wybranego magazynu,
* Przywracanie pliku danych klienta pocztowego Thunderbird,
* Przywracanie danych Microsoft 365 do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku: pst, mbox.
 |
| Backup: | * Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla:
	+ Systemów operacyjnych:
		- Debian: 9+,
		- Ubuntu: 16.04+,
		- Fedora: 29+,
		- centOS: 7+,
		- RHEL: 6+,
		- openSUSE: 15+,
		- SUSE Enterprise Linux(SLES): 12 SP2+,
		- Windows: 7, 8.1, 10(1607+),11
		- Windows Server: 2008 R2+,2016, 2022
	+ Środowisk wirtualnych:
		- Hyper-V,
* Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla Baz danych**:**
	+ - Microsoft SQL,
		- MySQL,
		- PostgreSQL,
		- Firebird,
		- Dowolnych innych przez podpięcie skryptów pre/post.
* Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:
	+ 128 bit,
	+ 192 bit,
	+ 256 bit.
* Kompresja danych wykonywana po stronie stacji roboczej
* Wykonywanie kopii zapasowej otwartych plików (VSS),
* System umożliwia uruchamianie skryptów przed i po backupie,
* System umożliwia uruchamianie skryptów po wykonaniu migawki VSS,
* System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów,
* Backup jednego oraz wielu dysków/całego systemu operacyjnego (Windows) ze wsparciem dla partycji MBR oraz GPT,
* Backup plikowy,
* Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe,
* Oprogramowanie umożliwia konsolidację wersji kopii zapasowych,
* Oprogramowanie ma pozwalać na backup zaszyfrowanych partycji.
 |

|  |
| --- |
| **Macierz dyskowa NAS - 1 sztuka** |
| Wymagania ogólne | 1. Do instalacji w standardowej szafie RACK 19 wraz z kompletem szyn do montażu w szafie Rack. Całość rozwiązania nie może zajmować więcej niż 2U w szafie RACK. Wraz z urządzeniem muszą być dostarczone elementy montażowe umożliwiające instalację we wszystkich zatokach dysków twardych (kieszenie, śrubki montażowe)
2. Minimum 8 wewnętrznych kieszenie na dyski, w których można zastosować dyski HDD oraz SSD z interfejsem SATA 6Gb/s
3. Minimum 2 lata gwarancji producenta.
 |
| Wydajność obliczeniowa CPU | Zainstalowany procesor minimum czterordzeniowy, wielowątkowy, ze wsparciem dla wirtualizacji, x86, 64bit., minimalne taktowanie 2.2 GHz.  |
| Pamięć RAM | Minimum 32GB |
| RAID | Wymagana obsługa: RAID 0, RAID 1, RAID 10, RAID 5, RAID 6, RAID 50, RAID 60 |
| Szyfrowanie danych | Z wykorzystaniem AES-NI |
| Porty | 1. Ethernet: minimum 4x Gigabit Ethernet, 2xSFP+ (10GbE)
2. Porty USB: minimum 2porty USB 3.2
3. Sloty PCI: Minimum 3x PCIe
4. Minimum 2 wkładka światłowodowe 10G dla kabla wielomodowego i patch cord umożliwiający podłączenie NAS z przełącznikiem sieciowym.
 |
| Cache SSD | Urządzenie musi wspierać technologię SSD Cache pozwalającą rozbudować pamięć podręczną odczytu z wykorzystaniem nośników SSD |
| Interfejs | Graficzny, pozwalający na wielowątkową równoległą pracę uruchomionych procesów/aplikacji, minimum w językach angielskim i polskim. System musi wspierać (obsługiwać) wirtualizację oraz konteneryzację, tj. musi być możliwość uruchamiania maszyn wirtualnych bezpośrednio na urządzeniu jak i uruchamiania aplikacji kontenerowych |
| Wsparcie dla protokołów: | SMB, AFP, iSCSI, FibreChannel, NFS, FTP, SNMP, VPN |
| Hypervisor | Zgodność z VMware, Hyper-V |

|  |
| --- |
| **Dyski do macierzy dyskowej NAS – 12 szt.** Doposażenie macierzy nowo dostarczonej dyskowej w dyski.  |
| 1. Pojemność min. 4TB
2. Dedykowane do pracy 24/7 w oferowanej macierzy dyskowej NAS,
3. Muszą znajdować się na liście kompatybilności producenta nowego urządzenia NAS.
4. min. 64MB cache.
5. MTBF na poziomie min. 1 mln godzin technologia wykrywania drgań w środowiskach RAID wielodyskowych.
6. Wymiana dysków może być dokonywana przez klienta.
7. Minimalna średnia szybkość prędkość: 180MB/s, Interfejsu 6 Gb/s
8. Gwarancja producenta min. 3 lata
 |

|  |
| --- |
| **Przełącznik sieciowy dostępowy warstwy L2 – 1 szt.**Zarządzalny przełącznik będzie zainstalowany w pokoju, gdzie pracują pracownicy biurowi, więc powinien być bezszelestny. Przełącznik sieciowy kompatybilny z przełącznikiem sieciowym warstwy L3. |
|

|  |
| --- |
| 1. Minimalna ilość portów elektrycznych: 24x 10/100/1000Base-T RJ45 +
2. Minimalna ilość portów światłowodowych: 2x 1/10GBase SFP+
 |
| 1. Minimalna matryca Przełączająca: 128 Gb/s
 |
| 1. Minimalna przepustowość: 95 Mp/s
 |
| 1. Minimalny bufor pakietów: 1,5 MB
 |
| 1. Ramki jumbo: 10 K
 |
| 1. Minimalna tablica MAC: 16 K
 |
| 1. Minimalna tablica Multicast MAC: 1 K
 |
| 1. Tablica ACL: 384
 |
| 1. Minimalna ilość Interfejsów VLAN (IP): 512
 |
| 1. Dodatkowe informacje: Tablica adresów MAC współdzielona dla unicast i multicast (w proporcji 1:1)
 |
| 1. Funkcje podwyższonej dostępności: IEEE 802.1D STP/802.1w RSTP/802.1s MSTP, IEEE 802.3ad LACP, Virtual Cable Testing, DDM, LLDP / LLDP-MED, Loop guard, ERPS (ITU-T G.8032)
 |
| 1. Kontrola Ruchu: 802.1Q VLANs, Port-based VLAN, Protocol-based VLAN, IP subnet based VLAN, Voice VLAN, Mac VLAN, LACP algorithm of source/destination IP (load balance), GVRP, 802.1ad Vlan Stacking (QinQ), Flexible QinQ
 |
| 1. Bezpieczeństwo: Layer 2 MAC filtering, BPDU Tunnel, Login authentication and authorization by RADIUS and TACACS+, TACACS+ accounting/ auditing, SSH v1/v2, DHCP/DHCPv6 snooping, IP/IPv6 Source Guard, Port security, IEEE 802.1x port-based / mac-based
 |
| 1. QoS: 802.1p Priority Queues per Port, 802.1p Queuing method, Trusted COS/TOS/IP Precedence/DSCP/Port number, Broadcast Storm Control, Rate Limiting, port based, Strict priority, Weighted Deficit Round Robin, Weighted Random Early Detection, Strict priority in Weighted Deficit Round Robin
 |
| 1. L2/L3 Multicast: Multicast VLAN, IGMP v1,v2, v3, IGMP Query, IGMP Snooping (v1,v2,v3), IGMP Snooping Fast Leave (v2,v3), IPv6 MLD v1/v2 Snooping
 |
| 1. Warstwa 3 IPv6: IPv4/IPv6 Dual Protocol Stack, IPv6 address
 |
| 1. Zarządzanie: Port konsolowy RS-232 (RJ45), GUI (Web), Telnet, SNMP v1/v2c/v3, TFTP/FTP, Kopia zapasowa konfiguracji oraz jej przywracanie, Wielopoziomowy CLI, DHCP Client/Relay/Server, DHCP relay per VLAN, DHCP option 43/60/82, DHCPv6 option 37/38, DHCPv6 Relay/Server, SNTP / NTP, sFlow, Stack (VSF), Port Mirroring per IP/TCP/UDP, RSPAN, IEEE 802.3ah EFM, IEEE 802.1ag CFM
 |
| 1. MIB: RFC1066 - TCP/IP‐based MIB, RFC1213, 1157 - SNMPv2c/v3 MIB, RFC1493 - bridge MIB, RFC2674 - bridge MIB extension, RFC1643 - ethernet MIB, RFC1757 - RMON group 1,2,3,9, RFC2925 - Remote Management MIB, RFC2233 ‐ SMIv2 MIB
 |
| 1. Zasilanie: 230 V AC
 |
| 1. Maksymalny pobór mocy: ≤ 21 W
2. Urządzenie będzie pracować w podwieszanej szafie w pomieszczeniu biurowym, więc wymaga się, aby urządzenie było bezszelestne lub ciche umożliwiając pracę osobom znajdującym się w pobliżu urządzenia.
3. Gwarancja nie mniej niż 2 lata
4. Przełącznik musi zostać doposażony w 2 wkładki światłowodowe SFP+ dla kabla wielomodowego, który łączy budynki Zamawiającego
 |

 |

|  |
| --- |
| **Przełącznik sieciowy dostępowy warstwy L3 – 1 szt.**Zarządzalny przełącznik sieciowy tej samej marki co przełącznik sieciowy warstwy L2, ze względu na kompatybilność.Zamawiający opisując przełącznik sieciowy miał na uwadze przełącznik marki DCN S5750E-52X-SI-R2 lub równoważny. |
|

|  |
| --- |
| 1. klasyfikacja: Przełącznik dostępowy warstwy 3
 |
| 1. Minimalna ilość portów elektrycznych: 48x 10/100/1000Base-T
2. Minimalna ilość portów światłowodowych: 4x 1/10GBase-X SFP+
 |
| 1. Port zarządzający: 10/100Base-T RJ45 - Out of Band
 |
| 1. Matryca Przełączająca: 176 Gb/s
 |
| 1. Przepustowość: 131 Mp/s
 |
| 1. Bufor pakietów: 3 MB (2x 1,5 MB)
 |
| 1. Ramki jumbo: 10 K
 |
| 1. Tablica MAC: 16 K
 |
| 1. Tablica Multicast MAC: 4 K
 |
| 1. Tablica ACL: 1 K
 |
| 1. Tablica routingu: 1 K
 |
| 1. Tablica ARP: 4 K
 |
| 1. Ilość Interfejsów VLAN (IP): 1 K
 |
| 1. Dodatkowe informacje: Tablica adresów MAC współdzielona dla unicast i multicast (w proporcji 1:1), Tablica ACL współdzielona dla ACL wejściowych i wyjściowych (w proporcji 1:1), Tablica Routingu dla IPv4 współdzielona z IPv6 (w proporcji 4:1), Gwarancja nie mniej niż 2 lata.
 |
| 1. Funkcje podwyższonej dostępności: IEEE 802.1D STP/802.1w RSTP/802.1s MSTP, IEEE 802.3ad LACP, Virtual Cable Testing, DDM, LLDP / LLDP-MED, VRRP, Loop guard, ERPS (ITU-T G.8032)
 |
| 1. Kontrola Ruchu: 802.1Q VLAN, Port-based VLAN, Protocol-based VLAN, IP subnet based VLAN, Voice VLAN, Mac VLAN, Super VLAN, LACP algorithm of source/destination IP (load balance), GVRP, 802.1ad Vlan Stacking (QinQ), Flexible QinQ
 |
| 1. Bezpieczeństwo: Layer 2 MAC filtering, BPDU Tunnel, Login authentication and authorization by RADIUS and TACACS+, TACACS+ accounting/ auditing, SSH v1/v2, DHCP/DHCPv6 snooping, IPv4/IPv6 Source Guard, Port security, IEEE 802.1x port-based / mac-based
 |
| 1. QoS: 802.1p Priority Queues per Port, 802.1p Queuing method, Trusted COS/TOS/IP Precedence/DSCP/Port number, Broadcast Storm Control, Rate Limiting, port based, Strict priority, Weighted Deficit Round Robin, Weighted Random Early Detection, Strict priority in Weighted Deficit Round Robin
 |
| 1. L2/L3 Multicast: Multicast VLAN, IGMP (v1,v2,v3), IGMP Query, IGMP Snooping (v1,v2,v3), IGMP Snooping Fast Leave(v2,v3), PIM (DM/SM/SSM), anycast RP, IPv6 MLD v1/v2 Snooping
 |
| 1. Routing: Static route IPv4 / IPv6, RIP v1,v2 / RIPng, OSPF v2 / OSPF v3, BGP / BGP4+
 |
| 1. Warstwa 3 IPv6: IPv4/IPv6 Dual Protocol Stack, IPv6 address, IPv6 Tunneling
 |
| 1. Zarządzanie: Console Port RS-232 (RJ45), GUI (Web), telnet, SNMP, TFTP/FTP, Configuration backup and restore, Multilevel CLI, DHCP Client/Relay/Server, DHCP (Option 43/60/82), DHCPv6 (Option 37/38), DHCPv6 Relay/Server, SNTP / NTP, sFlow, RSPAN, ERSPAN, Cluster, Stack (VSF), IEEE 802.3ah EFM, IEEE 802.1ag CFM
 |
| 1. MIB: RFC1066 - TCP/IP‐based MIB, RFC1213, 1157 - SNMPv2c/v3 MIB, RFC1493 - bridge MIB, RFC2674 - bridge MIB extension, RFC1643 - ethernet MIB, RFC1757 - RMON group 1,2,3,9, RFC2925 - Remote Management MIB, RFC2233 ‐ SMIv2 MIB
 |
| 1. Zasilanie: 230 V AC
 |
| 1. Maksymalny pobór mocy: ≤ 50 W
2. Przełącznik musi zostać doposażony w 4 wkładki światłowodowe SFP+ dla kabla wielomodowego, który łączy budynki Zamawiającego
3. Do każdego z przełączników musi być dostarczony kable DAC łączący dwa porty SFP+ przełączników w jednej szafie. Kabel może być długości 1,5m.
 |

 |

**Część III: Sprzęt do umożliwienia bezpiecznej komunikacji bezprzewodowej:**

|  |
| --- |
| **Punkt WiFi – 4 szt.**Nowe urządzenia umożliwią bezpieczną komunikację WiFi z wykorzystaniem oddzielnych sieci SSID dla pracowników i oddzielnych dla petentów. Izolacja sieci odbędzie się poprzez sieci VLAN. Zamawiający opisując punkt WiFi miał na uwadze Ubiquiti Networks U6Lite lub równoważny.  |
| Interfejsy | 1. Minimum Wi-Fi 802.11ac
2. Minimum 1 port RJ-45 10/100/1000 (LAN)
 |
| Częstotliwość pracy | Dual-Band: 2,4 GHz i 5 GHz |
| Prędkość transmisji bezprzewodowej | Minimum 1200 Mb/s dla 5GHz i 300 Mbps dla 2.4GHz |
| Antena | Wewnętrzna |
| Zabezpieczenia transmisji bezprzewodowej | * AES
* TKIP
* 64/128-bit WEP
* WPA
* WPA2
* Obsługa przypisania min. dwóch sieci SSID do sieci VLAN
 |
| Zasilanie | 1. PoE
2. Do zestawu musi być dołączony zasilacz PoE w celu zasilenia Punktu bezprzewodowego
 |
| Dodatkowe informacje | 1. Obsługa wielu sieci SSID
2. Obsługa wielu sieci VLAN
3. Funkcja zbierania informacji na temat zakłóceń sieci 5 i 2.4 GHz
 |
| Dołączone akcesoria | * Kabel zasilający
* Zestaw do montażu naściennego lub sufitowego
* Adapter Gigabit PoE
 |
| Gwarancja  | Minimum roczna |

|  |
| --- |
| **Menadżer WiFi – 1 szt.**System centralnego zarządzania punktami WiFi. Zamawiający opisując punkt WiFi miał na uwadze Ubiquiti Networks UniFi Cloud Key Gen2 (UCK-G2-Plus) lub równoważny.  |
| Interfejsy | * RJ-45 10/100/1000,
 |
| Minimalne parametry | * Ośmiordzeniowy procesor
* Minimum Pamięć 2GB RAM
* Minimum możliwość zarządzania 15 punktami bezprzewodowymi jednocześnie bez potrzeby dokupywania licencji
* wyświetlacz na panelu przednim
* 32 GB pamięci eMMC
 |
| Wewnętrzna pamięć masowa | 1 TB 2.5" SATA HDDMożliwość rejestrowania obrazu z kamery |
| Zasilanie | 802.3af PoE lub QC 2.0 USB-CWymaga się dostarczenia zewnętrznego zasilacza PoE lub USB-C do zasilania Menadżerem |
| Konfiguracja | Minimum za pomocą wykorzystania Bluetooth oraz aplikacji mobilnej lub interfejsu WEB urządzenia |
| Gwarancja  | Minimum roczna |

**Część IV: Rozbudowa zabezpieczeń i zabezpieczenie sieci:**

|  |
| --- |
| **Firewall z systemem IDS/IPS** Zamawiający będzie łączyć tunel IPSEC VPN z obecnie posiadanym rozwiązaniem marki Stormshield. Urządzenia muszą mieć możliwość zestawienia tunelu IPSEC VPN oraz powinny być kompatybilne pod względem zarządzania i monitorowania.  |
| Obsługa sieci | 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4
2. Urządzenie ma posiadać wsparcie dla protokołu IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.
3. Urządzenie ma posiadać wsparcie dla mechanizmu SD-WAN
 |
| Funkcjonalności Firewall | 1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
4. Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów.
5. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia.
6. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).
7. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer Active Directory, LDAP.
 |
| Intrusion Prevention System (IPS) | 1. System detekcji i prewencji włamań (IPS) ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
2. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS musi zabezpieczać przed znanymi atakami i zagrożeniami.
4. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej.
6. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
7. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych).
8. Głęboka analiza protokołów musi obejmować protokoły przemysłowe, co najmniej MODBUS TCP i Profinet.
 |
| Ochrona antyspam | 1. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
2. Ochrona antyspam ma działać w oparciu o:
* białe/czarne listy,
* DNS RBL,
* heurystyczny skaner.
1. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.
2. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
 |
| Wirtualne sieci prywante (VPN) | 1. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
2. Odpowiednio kanały VPN można budować w oparciu o:
* IPSec VPN,
* SSL VPN
1. SSL VPN musi działać w trybach Tunel i Portal.
2. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPNwspółpracującego z oferowanym rozwiązaniem.
3. Urządzenie ma umożliwiać utworzenie i pracę tunelu IPSEC VPN z obecnie zainstalowanym u Zmawiającego firewallem marki Stormshield.
 |
| Filtr dostępu do stron WWW | 1. Urządzenie ma posiadać wbudowany filtr URL.
2. Filtr URL ma działać w oparciu o klasyfikację URL
3. Administrator musi mieć możliwość dodawania własnych kategorii URL.
4. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.
5. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:
* blokowanie dostępu do adresu URL,
* zezwolenie na dostęp do adresu URL,
* blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
1. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
2. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.
3. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.
4. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
5. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.
 |
| Uwierzytelnianie | 1. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:
* lokalną bazę użytkowników,
* usługę katalogową Microsoft Active Directory.
1. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory.
2. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.
 |
| Administracja łączami do internetu (ISP) | 1. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing) oraz SDWAN.
2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
* równoważenie względem adresu źródłowego,
* równoważenie względem połączenia.
1. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
2. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
3. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów.
4. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
 |
| Pozostałe usługi i funkcje rozwiązania | 1. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.
2. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.
3. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.
4. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS
5. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.
6. Urządzenie musi posiadać usługę DNS Proxy.
 |
| Administracja urządzeniem | 1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
2. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
3. Komunikacja może odbywać się na porcie innym niż https (443 TCP).
4. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
5. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS).
6. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX.
7. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji)
 |
| Raportowanie | 1. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.
4. System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów.
5. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu.
6. W ramach podstawowej licencji zamawiający powinien otrzymać opcjonalną możliwość rozbudowy korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
7. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy
 |
| Parametry sprzętowe | 1. Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać z wbudowanej pamięci flash.
2. Liczba portów Ethernet 10/100/1000Mbps – min. 8.
3. Przepustowość Firewalla – min. 3,5 Gbps
4. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 2,4 Gbps.
5. Przepustowość filtrowania Antywirusowego – min. 400 Mbps
6. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 600 Mbps.
7. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż 100.
8. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20.
9. Obsługa min. VLAN 64
10. Liczba równoczesnych sesji - min. 300 000 i nie mniej niż 18 000 nowych sesji/sekundę.
11. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
12. Do urządzenia należy dostarczyć kartę SD na logi o pojemności nie mniejszej niż 128 GB.
 |
| Gwarancja i licencje: | 1. Minimum roczne wsparcie i gwarancja producenta;
2. Urządzenie musi mieć licencję na możliwość rozpoznawania i zarządzania protokołami przemysłowymi;
 |

|  |
| --- |
| **System DLP dla 11 stacji roboczych**System do automatycznego zapobiegania utracie lub udostępnieniu danych. Dedykowany system Data Leak Prevention (DLP),ochrona przed wyciekiem danych ma uniemożliwić pracownikom niekontrolowane wynoszenie danych. System ma zabezpieczyć kluczowe pliki przed niepowołanym dostępem, zarówno wewnątrz jak i na zewnątrz organizacji, a także ostrzegać kadrę zarządzającą przed ryzykiem wycieku kluczowych danych. Wybrane pliki mają być szyfrowane. Ponadto system ma mieć możliwość kontroli wykorzystanie drukarek, aplikacji oraz wszelkich aktywności online. |
| Liczba komputerów objęta DLP | * 11
 |
| Wsparcie techniczne:* Świadczone jest w języku polskim,
* Zapewnia dostęp do aktualizacji oprogramowania,
* Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego,
* Obowiązuje przez okres minimum 36 miesięcy.
* System po ustaniu wsparcia musi działać bezprzerwowo dalej z pełnymi możliwościami zarządzania przez administratora, jednakże Zamawiający zgadza się na odebranie prawa dostępu do aktualizacji i wsparcia
1. Dostęp do dokumentacji instalatora i użytkownika
2. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10, Windows 11.
3. DLP nie powinno zbyt mocno obciążać pracy stacji roboczej.
4. Serwer administracyjny musi oferować możliwość instalacji na systemach co najmniej Windows Server 2016 lub 2022.
5. Wsparcie dla 32 i 64-bitowej wersji systemu Windows.
6. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
7. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL Express (darmowa wersja MS SQL Server).
8. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
9. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
10. Serwer administracyjny musi umożliwiać wykonanie instalacji/dezinstalacji zdalnej klienta na stacjach roboczych.
11. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym.
12. 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.
13. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
14. Administrator musi posiadać możliwość zarządzania bazą danych
15. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji
16. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu jak i ich usuwania.
17. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną Active Directory.
18. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej
19. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień:

a) monitorowania: wykorzystywanych aplikacji, odwiedzanych stron internetowych, wykorzystywanych plików, podłączonych urządzeń zewnętrznych oraz przesłanych i odebranych wiadomości e-mail, b) DLP: służące do oznaczania plików, tworzenia reguł dla plików wrażliwych, tworzenia białych i czarnych list urządzeń, c) Kontroli dostępu do stron internetowych oraz kontroli dostępu do aplikacji. 1. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym.
2. Serwer administracyjny musi umożliwiać zablokowanie uruchomienia trybu awaryjnego na stacji końcowej.
3. Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji.
4. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.
5. Administrator musi posiadać możliwość tworzenia własnych informacji dot. aplikacji oraz typów plików.
6. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF bądź XLS.
7. Konsola musi posiadać możliwość wysyłania alarmów dotyczących incydentów bezpieczeństwa.
8. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.
9. Serwer musi posiadać możliwość wysłania alertów co najmniej za pośrednictwem wiadomości email.
10. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.
11. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.
12. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku lub na wskazany adres(y) e-mail.
13. Serwer administracyjny musi posiadać wbudowany serwer SMTP udostępniony przez producenta oprogramowania.
14. Serwer administracyjny musi umożliwiać tagowanie plików na poziomie systemu plików lub na poziomie metadanych pliku.
15. Serwer administracyjny musi umożliwiać wykonanie zadania tagowania plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie istniejących plików z tagami.
16. Serwer administracyjny musi mieć możliwość tagowania plików wrażliwych w oparciu o:

a) aplikacje, z której zostały utworzone, b) lokalizację, c) adres URL, d) format pliku, e) zawartość pliku. 1. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno lokalnych jak i sieciowych.
2. Dla plików otagowanych, musi być możliwe utworzenie następujących reguł:

a) blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych, b) blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń, c) blokowanie oraz zezwalanie na drukowanie na określonych drukarkach, d) blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej, e) blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen, f) blokowanie oraz zezwalanie na wysyłanie do poczty webowej, g) blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury, zarówno za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi: • Dropbox, • Google Drive, • SharePoint, • OneDrive Business, • OneDrive Personal. h) blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów, i) blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu zdalnego, j) blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości, nagrywania na płyty oraz wirtualnego drukowania, k) uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikacje. 1. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
2. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
3. Serwer administracyjny musi umożliwiać określenie białych i czarnych list
4. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.
5. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
6. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
7. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika.
8. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.
9. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony 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 wyszukiwania danych.
3. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych od jakich zostanie uruchomione zadania tagowania.
4. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi i urządzeniami mobilnymi.
5. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz utylizacji sprzętu
6. Konsola webowa musi posiadać możliwość konfiguracji serwera SMTP.
7. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.
8. 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 porali do poszukiwania pracy |

|  |
| --- |
| **System antywirusowy z EDR dla 35 komputerów i 3 lata wsparcia**Pakiet bezpieczeństwa obejmujący antywirus chroniący przed atakami typu ransomeware, antyspyware, personal firewall typu EDR i EPP - służący wykrywaniu i reagowaniu na podejrzane aktywności na urządzeniach końcowych oraz centralna konsola.  |
| Serwer | 1. Oferowany system musi spełniać funkcjonalność współczesnych systemów EDR – Endpoint Detection & Response oraz EPP – Endpoint Protection Platform.
* W ramach funkcji EDR zaoferowany system musi mieć możliwość zautomatyzowanego blokowania, przeglądu zdarzeń i graficznej analizy ataku, powiadomienia w czasie rzeczywistym;
* W ramach funkcji EPP system musi mieć możliwość ochrony agenta i jego modułów, ochrony systemu, adaptacyjnej polityki bezpieczeństwa, analizę zachowania, kontrolę urządzeń zewnętrznych jak np. pendrive i WiFi.
1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2016 i 2022.
2. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL w tym, w wersji darmowej (Express).
3. Serwer administracyjny musi posiadać możliwość podłączenia 35 agentów oraz potencjalną możliwość rozbudowy o kolejne poprzez aktualizację licencji.
4. System musi mieć licencję typu wieczystego – tzw. perpetual.
5. Wsparcie musi być oferowane na okres minimum 3 lat.
6. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu konsoli lub przeglądarki www.
7. Serwer musi mieć możliwość zarządzania i przeglądania zdarzeń z wykorzystaniem interfejsu graficznego.
8. Serwer musi posiadać wbudowane reguły, po których wystąpieniu, nastąpi wyzwolenie zaplanowanego zdarzenia.
9. Administrator musi posiadać możliwość kopiowania reguł i edycji reguł dodanych przez producenta.
10. Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak:
* Możliwość monitorowania systemu bez blokowania celem rozpoznania wszystkich zdarzeń typu False Positives;
* Zapewniać proaktywną ochronę;
* Kontrolę WiFi;
* Kontrolę Bluetooth;
* Kontrolę pendrive USB;
* Kontrolę wolumenu dyskowego;
* Kontrolę połączeń sieciowych;
* Kontrolę urządzeń CD/DVD;
* Ochronę przed przepełnieniem buforów;
* Wykrycie eskalacji uprawnień;
* Ochronę przed działaniem aplikacji typu keylogging;
* Ochronę danych wrażliwych;
* Kwarantannę dla zainfekowanych komputerów;
* Współpracę z firewallem będącym w posiadaniu Zamawiającego marki Stormshield;
* Blokadę wybranych aplikacji;
* Zapewniać bezsygnaturową ochronę przed atakami typu ransomeware;
* Kontrolować dostęp do zasobów takich jak pliki i rejestr.
1. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych co najminiej SHA.
2. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu.
3. Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie filtrów.
4. System musi korzystać z bazy wiedzy o taktyce i technikach bazujących na wiedzy MITRE i ATT&ACK.
5. W momencie wykrycia ataku rozwiązanie zabezpieczające powinno dać możliwość oceny sytuacji poprzez dokładne zapoznanie się ze zdarzeniami przedstawionymi w sposób graficzny zawierającymi pełen kontekst poprzez prezentację wszystkich zdarzeń poprzedzających atak.
6. Możliwość eksportu zdarzeń za pomocą syslog do zewnętrznych systemów SIEM.
 |
| **Agent** | 1. Pełne wsparcie dla systemu Windows 7 SP1/ Windows 8.1/Windows 10, Windows 11 oraz Windows Server 2008 R2/2012 R2/2016/2019 i 2022.
2. Wsparcie dla 32 i 64-bitowej wersji systemu Windows.
3. Agent musi współpracować z systemem centralnego zarządzania i konsolą tego samego producenta.
4. W ramach wprowadzonych reguł administracyjnych użytkownik musi mieć możliwość wyświetlenia zarejestrowanych zdarzeń i ewentualnie wyświetlać stosowne powiadomienia, dotyczące czynności wykonanej przez agenta.
5. Połączenie agenta do serwera zarządzającego musi być szyfrowane.
6. Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane.
7. Agent, jeżeli zostanie tak skonfigurowany powinien być przezroczysty dla użytkownika.
 |
| **Inne** | 1. Jeżeli system EDR wymaga zmiany systemu antywirusowego będącego w posiadaniu Zamawiającego, to należy dostarczyć ten system w cenie rozwiązania.
2. System EDR nie może zbyt mocno obciążać pracy stacji roboczej.
 |

Ogólne wymagania:

Produkty muszą być fabrycznie nowe i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju.