Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Opis wdrożenia ochrony poczty:

- Instalacja w miejscu wyznaczonym przez Zamawiającego

Konfiguracja systemu ochrony poczty w tym:

- Interfejsów oraz adresacji IP
- Routingu
- Serwera czasu
- Domen oraz subdomen
- Profili antyspamowych, antywirusowych oraz content z blokowaniem plików exe
- Polityk IP oraz Recipient
- Integracja z LDAP (jeżeli istnieje serwer LDAP)
- Ograniczenie wielkości plików oraz wielkości wiadomości
- Zdefiniowanie czarnych i białych list

- przygotowanie dokumentacji powdrożeniowej będąca opisem stanu systemu na dzień zakończenia wdrożenia

Opis wdrożenia przełączników LAN:

- Instalacja w miejscu wyznaczonym przez Zamawiającego
- Aktualizacja przełącznika
- Konfiguracja snmp, ntp, ssh, stp, dostępu dla administratorów, stack.vlan

Opis wdrożenia systemu do zarządzania infrastrukturą IT:

- Instalacja, konfiguracja, profilowanie dostarczonego systemu
- Nadzór wdrożeniowy oraz szkolenie z dostarczonego systemu dla 2 administratorów

Wymagania dodatkowe dotyczące wdrożenia

Zamawiający wymaga, żeby Wykonawca dostarczający i wdrażający rozwiązanie posiadał zatrudnionych na etacie inżynierów posiadających następujące certyfikaty techniczne **(wykaz osób wymagany jako załącznik do umowy)**:

- Certyfikat techniczny wydany przez producenta dostarczonego rozwiązania ochrony poczty.
- Certyfikat techniczny wydany przez producenta dostarczonego rozwiązania storage.

PRZEDMIOT ZAMÓWIENIA OBEJMUJE 5 POZYCJI, w tym:

POZ. 1 – System do zarządzania infrastrukturą IT

1. Architektura / budowa

1.1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 2000 agentów jednocześnie.

1.2. System musi posiadać następującą architekturę:

1.2.1. Agent – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.

1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej). Pozwala na realizację pełnego zarządzania

systemem oraz zasobami, wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca mechanizmy raportowania (nie jest dopuszczalne stosowanie aplikacji webowej do przeglądania danych oraz innej aplikacji do wprowadzania/edycji danych).

1.2.3. Panel pracownika – aplikacja webowa dostępna dla pracowników i uruchamiana na komputerach pracowników udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach zgodnie ze specyfikacją opisaną poniżej.

1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z agentami.

1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.

1.2.6. Komponenty Agent, konsola administracyjna, serwer, baza danych muszą się aktualizować samodzielnie za pośrednictwem bezpiecznego połączenia z serwerów aktualizacji producenta systemu. Czas aktualizacji wszystkich komponentów systemu: serwer, konsola administracyjna, baza danych, agenci - nie może przekroczyć 24h od wydania przez producenta nowej wersji dowolnego komponentu. Agenci na komputerach muszą się zaktualizować samodzielnie w czasie nie dłuższym niż 1h od pobrania aktualizacji od producenta, przy czym aktualizacja agentów musi przebiegać w pełni automatycznie z wykorzystaniem funkcjonalności wbudowanej w system (bez użycia zewnętrznych narzędzi, np. MS Active Directory). W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie ze strony producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.

1.2.7. System musi w sposób w pełni automatyczny z wykorzystaniem serwera aktualizacji producenta aktualizować wzorce aplikacji, pakietów, pomoc i inne wbudowane bazy wiedzy.

1.2.8. Agent do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI.

1.2.9. Agent musi być dostępny dla administratora z poziomu webowej interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go od producenta), w postaci pliku msi gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów) w pliku msi.

1.2.10. Agent musi być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej.

1.2.11. System musi posiadać możliwość wygenerowania instalatora Agenta, który nie będzie wymagał uprawnień administracyjnych do zainstalowania.

1.2.12. Agent musi pracować w trybie niewidocznym dla użytkownika (usługa systemowa).

1.2.13. System powinien umożliwiać generowanie unikatowego identyfikatora agenta – wygenerowanego losowo i unikatowo (np. za pomocą mechanizmu typu GUID) lub w sposób powtarzalny dla danego komputera) na podstawie kombinacji parametrów wybranych przez użytkownika systemu spośród następujących: nazwy producenta BIOS, numeru seryjnego komputera, system UUID, nazwy komputera, dowolnego oraz losowego ciągu znaków.

1.2.14. Agent musi mieć definiowalny priorytet pracy (ABOVE_NORMAL, NORMAL, BELOW_NORMAL, IDLE), przy czym w każdym momencie administrator może automatycznie z poziomu konsoli administracyjnej systemu wydać polecenie zmiany tej konfiguracji na dowolnej grupie komputerów.

1.2.15. Agent musi wspierać do sześciu różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem i potrafić wykorzystać adres dostępny (na którym następuje połączenie z serwerem) w dowolnym momencie działania, bez konieczności restartu agenta.

1.2.16. System musi umożliwiać komunikację pomiędzy agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.

1.2.17. System musi mieć możliwość współpracy komponentów agent i serwer w taki sposób, aby serwer mógł współpracować ze wszystkimi poprzednimi wersjami agentów.

1.2.18. System musi mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem realizujące co najmniej: usuwanie zbędnych danych z systemu (dane z monitoringu uruchamianych aplikacji, uruchamianych procesów, odwiedzonych stron www, wydrukowanych dokumentów, indeksowanie bazy danych, kopie bezpieczeństwa przyrostowe i nieprzyrostowe, zmniejszanie bazy danych. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie. System musi prezentować historię przeprowadzonych konserwacji/utrzymania.

2. Wymagania systemowe

2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, Firefox, Chrome, Opera).

2.2. Agent musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.

2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11.

2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2012/2012R2/2016/2019/2022, Windows 10) oraz Java 8 (JRE lub JDK), Apache Tomcat 8+.

2.5. Baza danych musi działać na silniku Microsoft SQL Server 2012/2014/2016/2017/2019 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).

2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

3. Interfejsy

1.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.

1.2. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas import zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.

1.3. Import z Active Directory musi wspierać obsługę protokołów SSL oraz TLS.

1.4. Import z Active Directory musi umożliwiać podanie więcej niż jednej domeny.

1.5. System musi umożliwiać import użytkowników z zewnętrznego pliku CSV.

1.6. System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Interfejs dodatkowo musi umożliwiać importowanie użytkowników, struktur i licencji. Import musi umożliwiać pobieranie danych z dowolnego źródła danych o dowolnej strukturze danych z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje te same dane wcześniej zaimportowane.

1.7. System musi umożliwiać pobieranie danych z komputerów (wyników skanowania) metodą bezpośredniego połączenia, za pośrednictwem serwera pocztowego (MAIL), za pośrednictwem serwera HTTP/HTTPS.

4. Funkcjonalności systemu zarządzania infrastrukturą IT

4.1. Funkcjonalność agenta

4.1.1. System musi umożliwiać pełne zdalne zarządzanie agentami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania agenta, zmiany konfiguracji, uruchamiania skanowania,

przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego), uruchamiania i wyłączania polityk w obszarze bezpieczeństwa (DLP).

4.1.2. Agent musi mieć możliwość konfiguracji zakresu skanowania plików w oparciu o nazwę plików (z uwzględnieniem znaków wieloznacznych), lokalizację na konkretnym dysku, datę utworzenia pliku oraz wielkość

4.1.3. Agent musi mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej a konsola musi udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił.

4.1.4. Agent musi mieć budowę modułową – uniemożliwienie pracy jednego z modułów (np. w wyniku niekompatybilnego systemu operacyjnego, pracy programów firm trzecich, awarii sprzętowej) nie może blokować pracy całego Agenta.

4.1.5. Po wykryciu nieprawidłowości w pracy dowolnego z modułów Agent powinien podjąć samoczynną próbę jego naprawy i przywrócenia do działania.

4.2. Funkcjonalność konsoli administracyjnej.

4.2.1. Konsola musi być w pełni polskojęzyczna oraz dodatkowo posiadać wersje językowe niemiecką oraz angielską.

4.2.2. Interfejs konsoli musi być wyposażony w intuicyjne mechanizmy obsługi, musi zapewniać pełną obsługę funkcjonalną (dodawanie/modyfikacja/usuwanie).

4.2.3. Konsola administracyjna musi posiadać dashboardy – dashboard użytkownika, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie.

4.2.4. Dashboard użytkownika jest budowany samodzielnie przez użytkownika poprzez wybór szybkiego skrótu do dowolnego ekranu aplikacji lub wybór dowolnego widgetu.

4.2.5. Dashboard prezentujący parametry sieci zawiera widgety pogrupowane w kategorie: Czat, Gry, Peer to peer, Streaming, Usługa podstawowa, Usługa podstawowa (szyfrowana), Złośliwe oprogramowanie.

4.2.5.1.1. Lista monitorowanych usług: AIM/ICQ, Back Orifice, Bagle.B, Bagle.h, BGMP, BGP, BitTorrent, Blaster, Blizzard's Battle.net, Call of Duty, Dabber, DHCPv6 (client), DHCPv6 (server), Direct Connect, DNS, Doom, Emule, FTP (connection control), FTP (data port), FTPS (TLS/SSL)(connection control), FTPS (TLS/SSL)(data port), GameSpy Arcade, Gnutella, Gopher protocol, HTTP, HTTP Proxy, HTTPS, IMAP, IMAPS, IMAPv3, iperf, IRC, IRC, iSCSI, Jedi Knight: Jedi Academy, Kazza, Kerberos, Killing Floor, LDAP, LDAP (SSL), LDP, LogMeIn Hamachi, MMP, MPP, MS Exchange Routing, MS Media Server, MS SQL Server (monitor), MS SQL Server (server), MSDP, MSN, Mu Online, Mxit, MySQL, Nessus, NetBIOS (Datagram Service), NetBIOS (Name Service), NetBIOS (Session Service), NetBus, NFS, Niektóre gry firmy Blizzard, Nintendo Wi-Fi Connection, NNTP, NNTP (TLS/SSL), NTP, OpenVPN, POP3, POP3S, PostgreSQL, PPTP, Printer-IPP, Printer-RAW, Print-spooler, Radio internetowe, Rbot/Spybot, RDP, rsyns, RTCP, RTP, RTSP, Sasser, SFTP, SIP, SIP(TLS), SLP, SMB, SMTP,SMTPS, SNMP, SOCKS proxy, SSH, Steam, Structured Query Language (SQL) Services, Sub7, Symantec System Center agent, TACACS, TeamViewier, Telenet (TLS/SSL), Telnet, TSP, UUCP, VMware Server, VMware VAMI, WASTE, WHOIS, WINS, XMPP/Jabber, Yahoo,! Messenger.

4.2.5.1.2. Dla każdej z usług prezentowane są relacje do wszystkich komputerów zawierające połączenia: powolne, nieosiągalne, rozłączone i poprawne wraz z czasami połączeń.

4.2.6. Dashboard prezentujący informacje o bezpieczeństwie zawiera widgety zawierające informacje: błędy serwera zadań, błędy smart, komputery bez bitlockera, komputery bez połączenia z serwerem, komputery z błędami typu critical / error / warning, duży transfer sieciowy, komputery bez agenta, komputery offline, komputery online, komputery z naruszoną polityką dlp, komputery z nieaktualną polityką dlp, liczba administratorów lokalnych w systemie (online), logowanie w godzinach nocnych, monitorowanie transferu do dysków chmurowych , nieautoryzowana pamięć usb, nowe komputery, nowe urządzenia w sieci, oprogramowanie zabronione, przekroczone cal, przekroczone licencje, subskrypcje, które wygasły, systemy bez wsparcia, wielokrotne logowanie,

wysokie użycie cpu, wysokie użycie ram, zaległe szkolenia wideo, zaległe wiadomości elearning, zbyt mało miejsca na hdd, zmiany na kontach użytkowników, zmiany tcp/ip.

4.2.7. Konsola administracyjna musi być wyposażona w panel zawierający graficzne widgety prezentujące dane w postaci wykresu kołowego i słupkowego bądź w formie tabeli z danymi.

4.2.8. Dane na widgetach muszą być aktualizowane automatycznie nie rzadziej niż 1 raz/ godzinę lub w każdym czasie na życzenia użytkownika.

4.2.9. Widgety muszą być skojarzone dziedzinowo ze wszystkimi obszarami zarządzania infrastrukturą, a każdy obszar powinien być reprezentowany przez min. 5 widgetów (np. w obszarze zarządzania komputerami system powinien być wyposażony w widgety zawierające: ilość komputerów w ramach danego typu, ilość komputerów on/off-line, strukturę komputerów wg ilości pamięci RAM, ilość komputerów wg ilości wolnego miejsca na dysku, ilość komputerów wg dat ostatnich połączeń)

4.2.10. Z każdego widgetu można uzyskać szczegółową informację analityczną (listę z danymi składającymi się na wybraną wartość na widgecie).

4.2.11. System musi posiadać filtr roboczy, przeszukujący całą tabelę po zdefiniowanym słowie.

4.2.12. System musi umożliwiać i zapamiętywać w profilu użytkownika indywidualną personalizację interfejsu konsoli administracyjnej (wybór wyświetlanych kolumn, ich kolejność, język, definiowanie filtrów, kolejność sortowania, wyświetlane widgety, ich konfigurację i kolejność).

4.2.13. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą być dynamicznie filtrowane w oparciu o reguły utworzone przez dowolnego użytkownika systemu. Reguły muszą być zapamiętywane i dostępne w kolejnych sesjach oraz oparte co najmniej o: nazwę komputera, IP, rodzaj systemu operacyjnego, identyfikator agenta, strukturę organizacyjną, stan agenta (włączony/wyłączony), nazwę użytkownika zalogowanego, producenta sprzętu, dostawcę sprzętu, lokalizację komputera, dowolnie zdefiniowaną przez użytkownika wartość (np. kolor obudowy komputera). Użytkownik może wybrać za jednym razem więcej niż jedną regułę. Zmiana wybranej reguły powoduje aktualizację wyświetlonego widoku.

4.2.14. Dane prezentowane na wszystkich widokach/zakładkach w systemie muszą mieć możliwość filtrowania kolumnowego.

4.2.15. System musi umożliwiać definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, dodawanie, usuwanie, modyfikowanie, wydruk) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, musi być wyposażony w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku powoduje ukrycie opcji.

4.2.16. Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie traci prawa do korzystania z konsoli administracyjnej systemu.

4.2.17. Konsola musi umożliwiać wykonywanie poszczególnych poleceń na wielu rekordach, w szczególności na wszystkich rekordach, również tych, które nie są widoczne w konsoli w ramach jednej strony (zaznacz wszystko).

4.2.18. Konsola administracyjna musi zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja agenta, stanu agenta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera.

4.2.19. Konsola musi umożliwić bezpośrednie przejście do witryny internetowej producenta z poziomu repozytorium producentów (o ile taka jest dostępna, np. DELL).

4.2.20. Konsola musi umożliwić bezpośrednie przejście do strony producenta zawierającej dodatkowe dane konfiguracyjne na temat konkretnego komputera w oparciu o Service Tag lub inny unikatowy identyfikator (np. Dell)

4.2.21. Konsola musi zawierać w sobie pełną dokumentację systemu, dokumentacja musi być na bieżąco aktualizowana poprzez automatyczne mechanizmy aktualizacji z serwera aktualizacji producenta.

4.3. Funkcjonalność panelu pracownika
4.3.1. Automatyczne uruchamianie panelu w momencie zalogowania użytkownika do systemu operacyjnego.
4.3.2. Zakres informacji w panelu jest definiowany przez administratora w formie schematów przypisywanych dla wybranych grup pracowników.
4.3.3. Panel pracownika użytkowany przez kierownika zawiera dodatkowo dane dostępne w panelach podległych pracowników w formie danych skumulowanych i analitycznych.
4.3.4. Wszelkie informacje udostępniane w panelu pracownika pogrupowane są w logiczne sekcje, z możliwością indywidulanego bądź grupowego włączania / wyłączania (ukrywania) sekcji.
4.3.5. Sekcje informacyjne panelu pracownika
4.3.5.1. Zalogowany użytkownik – imię i nazwisko, IP, nazwa komputera, informacje z AD – nazwa domenowa, nr telefonu, nr telefonu komórkowego, stanowisko
4.3.5.2. Dashboard
4.3.5.2.1. Moje zgłoszenia – zgłoszenia do wsparcia technicznego (nowe, otwarte, rozwiązane).
4.3.5.2.2. Mój komputer – wykorzystanie RAM, dysku, CPU.
4.3.5.2.3. Produktywność - czas zalogowania, aktywność, produktywność.
4.3.5.2.4. Baza wiedzy – najczęściej odwiedzane artykuły wsparcia technicznego.
4.3.5.2.5. Szkolenia - lista filmów szkoleniowych do zapoznania przez pracownika.
4.3.5.2.6. Wiadomości – lista ostatnich wiadomości przesłanych pracownikowi.
4.3.5.3. Sprzęt
4.3.5.3.1. Komputery przypisane do pracownika (nr seryjny, MAC, IP, data ostatniego logowania).
4.3.5.3.2. Komputery używane przez pracownika (nr seryjny, MAC, IP, data ostatniego logowania).
4.3.5.3.3. Urządzenia przypisane przez pracownika (nr seryjny, typ, IP).
4.3.5.3.4. Urządzenia używane przez pracownika (nr seryjny, typ, IP).
4.3.5.4. Oprogramowanie
4.3.5.4.1. Lista używanego oprogramowania (nazwa aplikacji, wersja, Produkcent, użycie 2 okresi ostatnich 3, 6, 12 miesięcy, data ostatniego uruchomienia).
4.3.5.5. Uprawnienia ACL
4.3.5.5.1. Uprawnienia do zasobów udostępnionych i lokalnych wraz z informacją o właścicielu folderu oraz rodzaju uprawnienia.
4.3.5.6. Informacja o czasie pracy
4.3.5.6.1. Lista otwartych sesji pracownika (data zalogowania, nazwa komputera, IP, rodzaj połączenia (LAN, NAT, VPN), czas zalogowania).
4.3.5.6.2. Lista ostatnich sesji użytkownika (początek, koniec, czas trwania sesji, nazwa komputera, IP)
4.3.5.6.3. Lista używanego oprogramowania (nazwa aplikacji, wersja, producent, data ostatniego uruchomienia, użycie aplikacji w ostatnich 3, 6, 12 miesiącach).
4.3.5.6.4. Aktywność użytkownika w aplikacjach (aplikacja, kategoria aplikacji, łączny czas korzystania, czas korzystania aktywnego, czas korzystania pasywnego).
4.3.5.6.5. Aktywność użytkownika w internecie (adres URL, informacja o stronie www – czy SSL, czy bezpieczna, czy zawiera przekierowania, czy znajduje się na liście CERT, czy znajduje się na liście stron hazardowych, kategoria strony jest bezpieczna), kategoria strony, czy strona jest produktywna, łączny czas korzystania, czas aktywności, czas pasywności).
4.3.5.6.6. Wydruki – lista wydrukowanych dokumentów – data, godzina, nazwa drukarki, nazwa dokumentu, ilość stron, wydruk kolorowy czy monochromatyczny, łączny koszt wydruku).
4.3.5.7. Wsparcie techniczne
4.3.5.7.1. Formularz zgłoszenia awarii.
4.3.5.7.2. Informacja o wszystkich dokonanych zgłoszeniach.
4.3.5.7.3. Dostęp do bazy wiedzy.
4.3.5.8. Wiadomości
4.3.5.8.1. Lista wiadomości przesłanych do użytkownika (data, typ wiadomości, nadawca, treść).

4.3.5.9. Szkolenia

4.3.5.10. Lista pogrupowanych tematycznie szkoleń dedykowanych pracownikowi wraz z prezentacją stopnia zapoznania się.

4.4. Zarządzanie licencjami

4.4.1. System musi umożliwiać zarządzanie licencjami w ramach dowolnego elementu struktury organizacyjnej (dla wybranej struktury organizacyjnej pokazuje liczbę instalacji i liczbę licencji w danym modelu licencjonowania wraz z listą komputerów).

4.4.2. System musi dawać możliwość wykonywania (historia) wielu audytów legalności i zapamiętywać wyniki tych audytów w odniesieniu do systemów operacyjnych jak i aplikacji/pakietów, z uwzględnieniem segmentu struktury organizacyjnej.

4.4.3. Zarządzanie oprogramowaniem musi następować z podziałem na aplikacje i pakiety oprogramowania.

4.4.4. System musi pozwalać na zdefiniowanie dowolnej ilości tzw. „standardów oprogramowania", które definiują 3 kategorie oprogramowania: „oprogramowanie standardowe" – pozycje z tej listy są wymagane do zainstalowania obowiązkowo na każdym komputerze, „oprogramowanie dodatkowe" - pozycje z tej listy mogą być zainstalowane (nie jest to wymagane) a instalacja odbywa się na wniosek samego użytkownika lub jego przełożonego, „oprogramowanie nieokreślone" – oprogramowanie nie należące do żadnej z dwóch powyżej zdefiniowanych kategorii a zidentyfikowane na komputerze.

4.4.5. System umożliwia zdefiniowanie listy aplikacji zabronionych.

4.4.6. System umożliwia utworzenie schematów (kolekcji) oprogramowania zabronionego i w momencie pojawienia się ich na komputerze przystępuje do automatycznego odinstalowania w trybie cichym (bez interfejsu).

4.4.7. System musi umożliwiać zdefiniowanie dowolnej kategorii oprogramowania/pliku/procesu i samodzielnej przydzielenie oprogramowania/pliku/procesu do kategorii.

4.4.7.1. W oparciu o Machine learning system umożliwia analizę procesów oraz przypisanie im odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem uruchamianych procesów.

4.4.7.2. Automatyczne przypisanie kategorii do każdego uruchomionego procesu.

4.4.7.3. Niezależność od zewnętrznych dostawców bazy wzorców procesów.

4.4.8. System zbiera szczegółowe informacje o systemie operacyjnym (wersja, edycja, service pack, poprawki, data instalacji).

4.4.9. System umożliwia odczytywanie identyfikatorów i kluczy produktowych dla systemu operacyjnego oraz dowolnego oprogramowania, tam gdzie jest to tylko technicznie możliwe.

4.4.10. System wspiera następujące typy licencji: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, OEM Downgrade, Open, Select, MOLP Open Value (Company wide), MOLP Open Value (non-Company wide), MOLP Open Value Subscription, CAL, SAAS, Trial, Shareware, Cal Per User.

4.4.11. System automatycznie klasyfikuje i rozlicza licencje OEM dla systemów operacyjnych oraz licencje typu freeware dla aplikacji.

4.4.12. System musi pomijać w rozliczeniu licencje wygasłe (po terminie ważności) i informować administratora o wygasaniu licencji.

4.4.13. System musi umożliwiać wyróżnianie licencji zabezpieczonych kluczami sprzętowymi.

4.4.14. System automatycznie wskazuje liczbę posiadanych licencji oraz liczbę używanego oprogramowania (pokazuje braki oraz nadwyżki).

4.4.15. System automatycznie uwzględnia i rozlicza licencje typu Upgrade i Downgrade wg zdefiniowanych przez użytkownika reguł.

4.4.16. System prezentuje datę instalacji oprogramowania.

4.4.17. System umożliwia ewidencję licencji (data zakupu, cena, dostawca, nr faktury, typ licencji, klucz produktowy, identyfikator produktowy, data wygaśnięcia, nr dokumentu OT, nr

zapotrzebowania) poprzez rejestrację dokumentów źródłowych (faktur zakupu) z możliwością dołączenia dowolnych załączników z repozytorium.

4.4.18. System umożliwia przypisanie licencji do użytkownika i/lub komputera oraz udostępnia informację o licencjach zarejestrowanych i jednocześnie wolnych (nieprzypisanych).

4.4.19. System umożliwiać zbieranie informacji na temat uruchamianych aplikacji na inwentaryzowanych komputerach (m.in. czas uruchomienia, nazwa zalogowanego użytkownika, nazwa aplikacji). System musi posiadać mechanizm zabezpieczający przed powstaniem niekompletnych lub niewłaściwych zapisów w wyniku braku zasilania lub innych awarii inwentaryzowanego systemu/sprzętu).

4.4.20. System musi udostępniać informację o uruchamianych aplikacjach w okresie 3/6/12 miesięcy oraz udostępniać datę ostatniego uruchomienia.

4.4.21. System musi automatycznie wyliczać przybliżone oszczędności z zakupionych a nie zainstalowanych aplikacji, przybliżone oszczędności z zainstalowanych a niewykorzystanych licencji oraz przybliżone nakłady konieczne na uzyskanie pełnej legalności.

4.4.22. System musi umożliwiać podgląd historii zmian aplikacji i pakietów na komputerach.

4.4.23. System musi umożliwiać zdalne odinstalowanie oprogramowania na jednym bądź wybranych komputerach.

4.4.24. System musi udostępniać informacje o stopniu wykorzystania aplikacji / pakietów dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej.

4.4.25. System musi udostępniać informacje o stopniu wykorzystania oprogramowania typu web dla modeli licencjonowania oprogramowania typu CAL w podziale na analizę godzinową/dzienną/miesięczną w zadanym okresie czasu. W/w informacja winna być przedstawiona również w postaci graficznej.

4.5. Wzorce aplikacji i pakietów

4.5.1. System ma posiadać wbudowaną bazę wzorców dostawcy oprogramowania posiadającą co najmniej 3,5 tys. wzorców aplikacji, 1,3 tys. producentów, 21 tys. plików, 1,5 tys. wbudowanych treści umów licencyjnych różnych producentów oprogramowania.

4.5.2. System musi udostępniać informacje dotyczące plików, na podstawie których zidentyfikowana została dana aplikacja.

4.5.3. System musi prezentować informacje o ilości i dacie publikacji posiadanej bazy wzorców oprogramowania.

4.5.4. System musi posiadać możliwość definiowania własnych wzorców aplikacji i pakietów (składających się z aplikacji) w oparciu o definiowalne reguły rozpoznawania.

4.5.5. Własne wzorce aplikacji i pakietów muszą mieć pierwszeństwo w procesie rozpoznawania aplikacji i pakietów.

4.5.6. System musi mieć możliwość zamawiania bezpośrednio z poziomu konsoli administracyjnej u producenta systemu wzorców oprogramowania z możliwością wskazania dla jakiego komputera / komputerów wzorce mają być utworzone. Zamówione i utworzone przez Producenta wzorce muszą automatycznie (bez ingerencji administratora systemu) zostać zaimportowane do systemu.

4.5.7. System musi rozpoznawać wersję i edycję zainstalowanych pakietów Microsoft Office (tam gdzie jest to technicznie możliwe (np. Microsoft Office 2007 Professional, Microsoft Office 2007 Standard, Microsoft Office 2003 Standard itd.).

4.6. Inwentaryzacja sprzętu komputerowego

4.6.1. System musi umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem).

4.6.2. System musi zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation). Szczegółowość odczytywania danych musi być parametryzowana za pomocą definiowanego zapytania w standardzie WMI Query Language.

4.6.3. System ma umożliwiać skanowanie kości pamięci RAM (z podaniem jednoznacznej specyfikacji kości, typu, numeru seryjnego oraz informacji o taktowaniu).
4.6.4. System ma odczytywać informacje o zainstalowanych kościach pamięci: producent, numer seryjny (Serial Number), numer części (Part Number), rozmiar, częstotliwość, taktowania.
4.6.5. System musi mieć możliwość odczytywania danych z dowolnego miejsca rejestru systemowego. Musi istnieć możliwość łączenia (konkatenacji) kilku pozycji z różnych miejsc rejestru oraz możliwość automatycznego, rekurencyjnego wyszukiwania wartości podanego klucza począwszy od wskazanego miejsca w hierarchii kluczy rejestru.
4.6.6. System ma umożliwiać automatyczne skanowanie monitorów podłączonych do komputera (ze wskazaniem producenta, modelu, numeru seryjnego, przekątnej ekranu).
4.6.7. System ma umożliwiać skanowanie dysków twardych (z podaniem typu interfejsu, numeru seryjnego oraz informacji SMART).
4.6.8. System musi umożliwić budowanie powiadomień administracyjnych w oparciu o dowolne atrybuty tabeli SMART dysku.
4.6.9. System musi umożliwiać skanowanie uprawnień użytkowników oraz grup użytkowników wraz z informacją o uprawnieniach, czy konto jest włączone, zablokowane, czy wymagana jest zmiana hasła, czy hasło wygasa, czy hasło jest wymagane).
4.6.10. System prowadzi szczegółową ewidencję zmian konfiguracji sprzętu.
4.6.11. System udostępnia informacje o występowaniu plików na komputerach (nazwa, rozmiar, rodzaj, wielkość, lokalizacja, w przypadku plików wykonywalnych: wersja, producent).
4.6.12. System musi umożliwiać dokonanie klasyfikacji pliku wg dowolnie zdefiniowanych kategorii (np. audio, wideo, graficzne, erotyczne/pornograficzne, archiwa, wykonywalne.
4.6.13. System pozwala na zdalne trwałe (bez możliwości odzyskania) usunięcie dowolnego pliku/plików na dowolnie zdefiniowanej grupie komputerów.
4.6.14. System udostępnia informacje o zmianach w systemie plików (dodano plik, usunięto plik)
4.6.15. System umożliwia dodawanie notatek do każdej pozycji sprzętu.
4.6.16. System musi umożliwiać ewidencję zdarzeń serwisowych dowolnego typu (np. naprawy sprzętu, wymiany części).
4.6.17. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium.
4.6.18. System umożliwia samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów (przyjęcie, przekazanie do użytkowania, likwidacja).
4.7. Inwentaryzacja urządzeń podłączanych do komputera
4.7.1. System automatycznie identyfikuje i klasyfikuje urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.
4.7.2. System pozwala na automatycznie lub ręczne przypisanie podłączonego urządzenia do komputera oraz użytkownika.
4.7.3. System ewidencjonuje historię podłączanych urządzeń zewnętrznych w zakresie: komputer, data, godzina, kto podłączył, czy urządzenia było podłączane na innym komputerze, czy urządzenie było podłączane przez innego użytkownika).
4.8. Identyfikacja środowisk wirtualizacji
4.8.1. System musi być wyposażony w skaner środowisk wirtualizacji Hyper-V oraz VMware.
4.8.2. Skaner środowisk wirtualizacji musi być w pełni programowalny, musi obsługiwać wiele środowisk wirtualizacji oraz dowolną ilość atrybutów logowania (login, hasło).
4.8.3. Skaner środowisk wirtualizacji musi być wyposażony w programowalny harmonogram skanowania.
4.9. Inwentaryzacja urządzeń innych niż komputery
4.9.1. System musi umożliwiać inwentaryzację manualną (ewidencję) sprzętu innego niż komputery: np. drukarki, switche, routery, monitory, pamięci masowe itp.
4.9.2. System musi być wyposażony we wbudowany, konfigurowalny w zakresie IP oraz portów, pracujący zgodnie z harmonogramem skaner SNMP. Skaner musi wykryć typ urządzenia na danym

IP/porcie i zwracać podstawowe informacje o tym urządzeniu (nazwa, producent, opis). Skaner musi obsługiwać SNMP w wersji 1/2c/3.

4.9.3. Skaner SNMP musi kojarzyć (łączyć) zinwentaryzowane urządzenia (np. komputery, drukarki) z danymi uzyskanymi w procesie skanowania IP/port.

4.9.4. System musi zbierać informacje o jakości połączenia:

4.9.4.1. Czas odpowiedzi serwisów (usług) podawany w milisekundach:

4.9.4.1.1. Średni czas odpowiedzi.

4.9.4.1.2. Minimalny czas odpowiedzi.

4.9.4.1.3. Maksymalny czas odpowiedzi.

4.9.4.2. Ilość dostarczonych informacji – pakietów dostarczonych, straconych oraz procent strat.

4.9.5. System musi być wyposażony we wbudowany, konfigurowalny skaner sieci, pozwalający na monitorowanie aktywnych usług oraz zweryfikowanie czy znalezione skanerem komputery posiadają agenta, a w przypadku, gdy takiego agenta nie posiadają powinien umożliwić zdalną instalację agenta.

4.9.5.1. Posiada niezwłoczną i automatyczną identyfikację podłączonych urządzeń do sieci

4.9.5.2. Baza wzorców musi zawierać ponad 100 monitorowanych portów i usług.

4.9.6. System musi posiadać możliwość generowania map sieci bazujących na danych zebranych ze skanowania sieci.

4.9.6.1. System musi umożliwiać generowanie map według dowolnych filtrów użytkownika.

4.9.7. System umożliwia wprowadzanie dowolnych notatek oraz zdarzeń serwisowych.

4.9.8. System musi monitorować zmiany ewidencyjne i ruchy sprzętu.

4.9.9. System musi umożliwiać przypisanie urządzenia do użytkownika, ewidencję napraw, gwarancji.

4.9.10. System musi mieć możliwość przypominania o upływającym terminie gwarancji.

4.9.11. System musi pozwalać na dołączanie do urządzeń dokumentów z repozytorium wewnętrznego systemu.

4.9.12. System udostępnia informację o wartości wprowadzonego sprzętu.

4.9.13. System musi umożliwiać samodzielną definicję, ewidencję oraz wydruk wszelkiego typu protokołów oraz zapewniać automatyczną numerację tych dokumentów zapewniającą unikatowość.

4.9.14. System musi pozwalać na kopiowanie (duplikację) dowolnego urządzenia dowolną ilość razy.

4.9.15. System musi pozwalać na ewidencję umów utrzymaniowych (SLA) w odniesieniu do zaewidencjonowanych licencji oraz urządzeń w zakresie co najmniej: nazwa, okres, data dokumentu, numer dokumentu, dostawca, osoba kontaktowa, wartość, opis, warunki oraz umożliwiać dołączenie dowolnej ilości załączników z repozytorium i powiązanie umowy utrzymaniowej z dowolną ilością zasobów (urządzenia, licencje).

4.10. Ochrona danych (DLP)

4.10.1. System automatycznie tworzy listę podłączanych do komputerów urządzeń USB.

4.10.2. System automatycznie klasyfikuje podłączane urządzenia (pamięć masowa, pendrive, aparat fotograficzny, urządzenie multimedialne itp.)

4.10.3. System umożliwia uzyskanie informacji kto, kiedy i na jakim komputerze posługiwał się urządzeniem zewnętrznym, pozwalając na jego jednoznaczne zidentyfikowanie.

4.10.4. System umożliwia utworzenie listy urządzeń USB dozwolonych do stosowania - tzw. białej listy urządzeń USB.

4.10.5. System ma możliwość zidentyfikowania urządzenia USB i wprowadzenia go do systemu za pośrednictwem konsoli administracyjnej oraz wbudowanego do konsoli oprogramowania/skryptu, pozwalając na zidentyfikowanie jednocześnie wielu urządzeń USB (multiplekser USB).

4.10.6. System musi umożliwiać zdefiniowanie reguł stanowiących podstawę użytkowania urządzeń USB (dozwolone/niedozwolone) na inwentaryzowanych komputerach wg kryteriów: użytkownik, dzień tygodnia, okres (data od, godzina od, data do, godzina do), urządzenie USB, komputer, data obowiązywania reguły.

4.11. Szyfrowanie dysków wewnętrznych.

4.11.1. System musi identyfikować partycje dysków twardych zaszyfrowane BitLockerem.

4.11.2. System musi posiadać wbudowane mechanizmy do masowego zdalnego szyfrowania BitLockerem i wspierać metody XTS_AES_256, XTS_AES_128, AES_256, AES_128 oraz typy zabezpieczeń TPM+Pin, TPM, Passphrase.

4.11.3. Ochrona danych na budowanych dyskach twardych musi być realizowana przez silne szyfrowanie całej zawartości dysku/dysków z wykorzystaniem MS API Bitlocker oraz umożliwiać uwierzytelnianie użytkownika przed uruchomieniem startu systemu operacyjnego ze wsparciem metod silnego uwierzytelnienia.

4.11.4. Ochrona danych przez szyfrowanie całej zawartości dysku oznacza, że szyfrowaniu podlegają wszystkie informacje zapisane na dysku twardym (łączenie z system operacyjnym, sterownikami, zainstalowanymi programami, danymi itp.).

4.11.5. Funkcjonalność szyfrowania / deszyfrowania nie może być realizowana w oparciu o dodatkowego agenta na stacji roboczej lecz musi być integralnym rozwiązaniem oferowanego systemu.

4.11.6. System musi umożliwiać zdalne szyfrowanie / deszyfrowanie partycji systemowych oraz niesystemowych oraz prezentować w konsoli administracyjnej bieżący postęp procesu.

4.11.7. Szyfrowanie partycji niesystemowych polega na wprowadzeniu przez użytkownika hasła.

4.11.8. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika komputera i może być realizowany w czasie jego pracy na komputerze. Szyfrowanie nie może być zostać wyłączone przez użytkownika.

4.11.9. Proces szyfrowania może być zatrzymany podczas hibernacji oraz wyłączenia systemu ale jest kontynuowany po wzbudzeniu / włączeniu komputera.

4.11.10. System przechowuje klucze szyfrujące w konsoli administracyjnej, przy czym klucze są dostępne po dodatkowym uwierzytelnieniu administratora.

4.11.11. System musi umożliwiać szyfrowanie / deszyfrowanie komputerów w sieci lokalnej oraz poza NATem.

4.12. Szyfrowanie dysków zewnętrznych USB.

4.12.1. System musi identyfikować partycje dysków zewnętrznych zaszyfrowane BitLockerem.

4.12.2. System musi posiadać wbudowane mechanizmy do masowego zdalnego szyfrowania / deszyfrowania BitLockerem i wspierać metody XTS_AES_256, XTS_AES_128, AES_256, AES_128 oraz typ zabezpieczeń Passphrase.

4.12.3. Ochrona danych na zewnętrznych urządzeniach USB musi być realizowana przez silne szyfrowanie całej zawartości dysku z wykorzystaniem MS API Bitlocker oraz umożliwiać uwierzytelnianie użytkownika przed dostępem do danych ze wsparciem metod silnego uwierzytelnienia.

4.12.4. Funkcjonalność szyfrowania / deszyfrowania nie może być realizowana w oparciu o dodatkowego agenta na stacji roboczej lecz musi być integralnym rozwiązaniem oferowanego systemu.

4.12.5. Szyfrowanie partycji urządzeń USB polega na wprowadzeniu przez użytkownika hasła.

4.12.6. System musi umożliwiać zdalne szyfrowanie / deszyfrowanie partycji urządzeń USB oraz prezentować w konsoli administracyjnej bieżący postęp procesu.

4.12.7. Proces szyfrowania odbywa się w sposób niewidoczny dla użytkownika komputera i może być realizowany w czasie jego pracy na komputerze. Szyfrowanie nie może być zostać wyłączone przez użytkownika.

4.12.8. System przechowuje klucze szyfrujące w konsoli administracyjnej, przy czym klucze są dostępne po dodatkowym uwierzytelnieniu administratora.

4.13. Zdalna administracja komputerami

4.13.1. System ma automatyczne wykonywać dowolne polecenia na dowolnych komputerach: wykonywanie poleceń powłoki, uruchamianie aplikacji, instalacja/deinstalacja oprogramowania,

zmiany w rejestrach systemowych (dodawanie, usuwanie, modyfikowanie), usuwanie oraz kopiowanie plików i folderów, dostarczanie wyników zwróconych przez wykonane zadanie do bazy danych i prezentowanie ich w konsoli zarządzającej, możliwość wykonywania zadań z uprawnieniami dowolnego użytkownika.

4.13.2. System musi posiadać wbudowany skaner wyposażony w harmonogram skanowania umożliwiający wykrywanie (rozpoznawanie) komputerów z technologią Intel VPro/AMT wraz z identyfikacją IP technologii Vpro, portu VPro oraz wersji Vpro.

4.13.3. System musi umożliwiać zarządzanie komputerami z technologią Intel vPro, w tym: Serial Over LAN, zdalne włączanie, wyłączanie komputera, zdalna konfiguracja BIOS, uruchomienie zdalnie komputera przy użyciu obrazu ISO lub IMG znajdującego się w dowolnej lokalizacji.

4.13.4. System ma umożliwiać połączenie się z wybranym komputerem w trybie graficznym (od VPro v.6).

4.13.5. System musi umożliwiać za pomocą technologii Ultra VNC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalacja oprogramowania, poprawek i aktualizacji (service pack, patch).

4.13.6. System umożliwia zdalne podłączenie do wielu komputerów jednocześnie i podgląd oraz operowanie na pulpitach tych komputerów w technologii Ultra VNC.

4.13.7. System musi umożliwiać uruchomienie do 6 sesji Ultra VNC na jednym ekranie.

4.13.8. System musi umożliwiać uruchomienie sesji Ultra VNC w trybie podłączenia się do obecnie zalogowanego użytkownika oraz w trybie RDP (wylogowania użytkownika i przejęcia dostępu).

4.13.9. System musi posiadać predefiniowane zadania (polecenia) możliwe do wykonania zdalnie – niezwłocznie lub zgodnie z harmonogramem o funkcjonalnościach typowego harmonogramu windows; zadania powinny być podzielone na typy: administracyjne, bezpieczeństwo, konserwacyjne a użytkownik może utworzyć dowolny nowy typ zadania.

4.13.10. Minimalne zadania predefiniowane: wyświetlanie aktywnych połączeń sieciowych, czyszczenie buforu DNS, pobranie listy zalogowanych użytkowników, ping, tracert, pobranie listy procesów, wyłączenie/włączenie komputera, wyłączenie/włączenie usługi, wyłączenie/włączenie/restart zapory windows, włączenie usługi Windows Update, pobranie zmiennych środowiskowych, opróżnienie kosza, usunięcie plików tymczasowych, wymuszenie sprawdzenia dostępności aktualizacji Windows Update, wymuszenie aktualizacji zasad grup (AD), konserwację dysku twardego.

4.13.11. Każde wykonanie zadania musi mieć odzwierciedlenie w statusie wykonania zadania (poprawne, z błędem) oraz udostępniać informację zwrotną o przebiegu wykonania (godzina, data, status).

4.13.12. System musi umożliwiać zdefiniowanie dowolnego własnego zadania z poziomu konsoli administracyjnej z wykorzystaniem poleceń cmd, windows powershell. System posiada co najmniej 70 predefiniowanych poleceń.

4.13.13. System musi umożliwiać zdalne połączenia do wielu komputerów jednocześnie, podgląd i operowanie na pulpitach tych komputerów w technologii WEBRTC.

4.13.14. System musi umożliwiać za pomocą technologii WEBRTC: przejęcie ekranu, klawiatury i myszki użytkownika, zdalne uruchamianie aplikacji, zarządzanie usługami i restart komputera, zdalną instalację oprogramowania, poprawek i aktualizacji (service pack, patch).

4.13.15. System musi umożliwiać poprzez technologię WEBRTC zdalne zarządzanie plikami (tworzenie, kopiowanie, usuwanie, przesyłanie) i wykorzystanie wiersza poleceń (cmd) oraz powershell bez konieczności podłączenia do komputera.

4.13.16. System musi umożliwiać nagrywanie sesji połączeń WEBRTC jak i nawiązywanie komunikacji z użytkownikiem podczas sesji (czat).

4.13.17. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.

4.13.18. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.

4.14. Automatyzacja

4.14.1. System ma mieć możliwość ustalania harmonogramu, zgodnie z którym uruchamiane są czynności konserwacyjne, naprawcze, porządkujące.

4.14.2. Harmonogram musi mieć możliwość ustalenia częstotliwości wykonywania danej czynności (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych, a także zatrzymania/uruchomienia harmonogramu uruchomienia dla każdej z czynności.

4.14.3. System musi mieć możliwość definiowania czynności wykonywanych automatycznie.

4.14.4. System musi być wyposażony w następujące mechanizmy automatyzacji: wykonywanie kopii bezpieczeństwa bazy danych, identyfikacja aplikacji i pakietów, porządkowanie bazy danych / odbudowa indeksów, usuwanie nadmiarowych danych w bazie danych, usuwanie zewnętrznych plików (logów).

4.14.5. System musi być wyposażony w mechanizmy informowania - wysyłania komunikatów (alerty) o: zasobach zakazanych (pliki erotyczne i pornograficzne), zasobach multimedialnych (pliki multimedialne), nowych komputerach w bazie danych, braku skanowania komputerów, brakach w licencjach, niewłaściwych datach systemowych komputerów, urządzeniach bez użytkowników, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, wygasaniu serwisu lub licencji, przekroczeniu wielkości bazy danych, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu sieci, nadmiernym obciążeniu sieci na komputerze, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku, upływającej gwarancji,

4.14.6. System musi wspierać obsługę dowolnych poleceń powłoki na stacjach roboczych (kopiowanie plików, usuwanie plików, przenoszenie plików, zmiana ustawień systemu, wykonywanie programów, instalacja oprogramowania, instalacja poprawek itp.).

4.14.7. System musi umożliwić wykonanie poleceń z uprawnieniami dowolnego użytkownika (Uruchom jako)

4.14.8. System musi umożliwiać tworzenie zadań cyklicznych dla komputerów.

4.14.9. Obsługa zadań cyklicznych musi następować w cyklu dziennym: co n dni, w każdy dzień powszedni, nowe zadanie n dni od wykonania, tygodniowym: w wybrane dni co n tygodni, nowe zadanie n tygodni od wykonania, miesięcznym: co x miesięcy n-tego dnia, pierwszy/drugi/trzeci/czwarty/ostatni poniedziałek/wtorek/środa/czwartek/piątek/sobota/niedziela/dzień wolny/dzień powszedni co n miesięcy, nowe zadanie n miesięcy od wykonania, rocznym: n dzień w wybranym miesiącu, w pierwszy/drugi/trzeci/czwarty/ostatni, w dowolny dzień tygodnia, dzień wolny/dzień powszedni wybranego miesiąca, nowe zadanie n lat od wykonania.

4.14.10. System musi obsługiwać zadania cykliczne: bez daty końcowej, z końcem cyklu po n wystąpieniach, z końcem cyklu w określonej dacie.

4.15. Zarządzanie magazynem IT

4.15.1. System musi umożliwiać obsługę magazynu IT.

4.15.2. System musi umożliwiać obsługę dowolnej ilości magazynów w różnych lokalizacjach.

4.15.3. System musi umożliwiać obsługę dokumentów PZ, WZ, MM+, MM-, LI.

4.15.4. System musi prowadzić ewidencję materiałów w magazynach w oparciu o metodę FIFO (pierwsze przyszło pierwsze wyszło).

4.15.5. System musi umożliwiać obsługę kodów kreskowych dla materiałów w magazynach.

4.15.6. System musi udostępniać informację o wartościach materiałów w poszczególnych magazynach, stanach materiałów w magazynach, dokumentach dotyczących danego materiału w dowolnym magazynie.

4.16. Repozytorium

4.16.1. Konsola administracyjna musi być wyposażona w repozytorium dokumentów dowolnego typu.

4.16.2. Repozytorium musi umożliwiać: dodawanie nowych dokumentów dowolnego typu, przeszukiwanie, oznaczanie dokumentów (znaczniki TAG) więcej niż jednym znacznikiem, podgląd dokumentów, dołączanie dokumentów z repozytorium w dowolnym miejscu systemu, uzyskanie informacji w jakich miejscach systemu dany dokument repozytorium występuje.

4.17. Kody kreskowe

4.17.1. System wspiera obsługę kodów kreskowych jedno i dwuwymiarowych.

4.17.2. System wspiera parametryzację kodu w zakresie wielkości graficznej kodu.

4.17.3. System pozwala w każdym momencie na zmianę typu i atrybutów kodu.

4.17.4. System informuje o błędzie generacji kodu, np. na skutek niewłaściwej długości wprowadzonego ciągu znaków w stosunku do danego standardu kodu.

4.17.5. Istnieje możliwość podglądu kodu oraz jednostkowego i masowego wydruku kodu / kodów.

4.17.6. System musi generować kody kreskowe (jedno i dwuwymiarowe) dla każdego zaewidencjonowanego urządzenia w standardzie wybranym przez użytkownika: aztec, codabar, code128, code39, dataMatrix, EAN128, EAN13, EAN8, interleaved2of5, ITF14, PDF417, POSTNET, qrcode, royalMailCBC, UPCA, UPCE, USPSIntelligentMail.

4.17.7. Obsługa kodów kreskowych nie może wymagać instalacji czcionek.

4.17.8. Parametry kodu kreskowego (wymiary, wielkość i typ czcionki) muszą być definiowalne.

4.17.9. System musi umożliwiać współpracę z zewnętrznymi czytnikami kodów.

4.18. System szkolenia pracowników za pomocą wiadomości.

4.18.1. System musi mieć możliwość zdefiniowania pakietów tekstowych (kontent) celem automatycznego wysyłania do urządzeń i użytkowników komputerów.

4.18.2. System musi posiadać predefiniowane szkolenia: „Klasyfikowanie informacji stanowiących tajemnicę przedsiębiorstwa", „Kontrola zabezpieczeń i obiegu informacji stanowiących tajemnicę przedsiębiorstwa", „Postępowanie w przypadku naruszenia tajemnicy", „Udostępnienie informacji stanowiących tajemnicę".

4.18.3. Formatowanie treści musi być zgodne z HTML.

4.18.4. System musi mieć możliwość edycji treści (zmiana kolejności, usuwanie, dodawanie nowych).

4.18.5. System musi mieć programowalny harmonogram wysyłania treści do dowolnej grupy odbiorców.

4.18.6. Użytkownik otrzymujący wiadomość musi być powiadamiany wizualne i dźwiękowo o otrzymaniu nowej wiadomości.

4.18.7. Użytkownik musi mieć możliwość natychmiastowego odczytania wiadomości lub jej odłożenia (na 10 minut, 1, 2 lub 4 godziny) celem późniejszego odczytania.

4.18.8. System musi posiadać zabezpieczenie (np. synchronizowany z serwerem znacznik czasowy) odporne na zmiany czasu na lokalnym komputerze (użytkownika) a pozwalające na jednoznaczne ustalenie daty i godziny dostarczenia i odczytania wiadomości.

4.18.9. System musi udostępnia historię przesyłania wiadomości i odczytywania wiadomości przez użytkowników.

4.18.10. System musi generować elektroniczną listę uczestników przeszkolonych (z odczytanym całym szkoleniem).

4.18.11. System musi posiadać możliwość eksportu / importu treści.

4.19. System szkolenia pracowników za pomocą filmów wideo.

4.19.1. System musi pozwalać na zdefiniowanie listy filmów szkoleniowych dla wybranej grupy pracowników za pomocą definiowalnego schematu szkoleniowego.

4.19.2. Proces szkolenia może być zdefiniowany jako szkolenia cykliczne – automatycznie powtarzane po upływie określonego czasu (np. 1 rok).

4.19.3. Każdy pracownik uzyskuje dostęp do filmów zdefiniowanych w przypisanym schemacie poprzez panel pracownika.

4.19.4. Panel pracownika zawiera listę filmów szkoleniowych dla danego pracownika pogrupowanych w zakładki tematyczne.

4.19.5. Filmy mogą być odtwarzane przez pracownika wielokrotnie przy czym panel informuje o stopniu przeglądnięcia (% zaawansowania) filmu przez pracownika.
4.19.6. System jest zabezpieczony przed przewijaniem filmu w taki sposób aby cały filmy został przez pracownika oglądnięty.
4.19.7. Pracownik może przerywać odtwarzanie filmu oraz odtwarzać film od dowolnego miejsca, przy czym system domyślnie wskazuje ostatnie miejsce przerwania oglądania.
4.19.8. Biblioteka filmów może być budowana przez administratora systemu.
4.19.9. Schematy filmów lub filmy w całości oglądnięte przez pracownika umożliwiają wydruk stosownego certyfikatu.
4.20. Monitorowanie drukarek sieciowych i wydruków
4.20.1. System musi posiadać możliwość ewidencji wszystkich generowanych wydruków niezależnie od miejsca ich generowania oraz typu drukarki (lokalna, sieciowa).
4.20.2. Ewidencja wydruków musi obejmować: nazwę i wielkość dokumentu, datę i godzinę wydruku, nazwę użytkownika drukującego, IP i nazwę komputera z którego dokonano wydruku, format dokumentu, informację i jedno bądź dwustronnym wydruku, informację o wydruku mono/kolor.
4.20.3. System dla każdego wydruku, dla każdej drukarki musi obliczać rzeczywisty koszt wydruku w oparciu o wbudowany cennik wydruków obejmujący cenę papieru (w zależności od formatu) oraz cenę materiałów eksploatacyjnych (toner, tusz) dla danej drukarki, typu wydruku, rozmiaru papieru.
4.20.4. System musi generować zestawienia pozwalające ustalić miejsca powstawania kosztów wydruków (komórki organizacyjne, użytkownicy) oraz stopień obciążenia poszczególnych urządzeń drukujących.
4.20.5. System musi prognozować ilość i koszt wydruków na wszystkich drukarkach w okresie kolejnych 3,6,12 miesięcy.
4.20.6. System musi pozwalać na grupowanie (kojarzenie) drukarek wg sterowników.
4.20.7. Dla każdej z drukarek SNMP system musi udostępniać informacje: nr seryjny, IP, MAC, bieżący status drukarki, całkowitą ilość wydrukowanych stron, ilość wydrukowanych stron od uruchomienia, błędy, alerty, dostępne porty, stan pokryw, interfejsów sieciowych, rodzaj i ilości pamięci całkowitej i wykorzystanej, informacje o poziomie materiałów eksploatacyjnych
4.21. Monitorowanie stron www
4.21.1. System musi posiadać możliwość monitorowania odwiedzanych stron www niezależnie od typu używanej przeglądarki internetowej.
4.21.2. Ewidencja otwieranych stron musi dotyczyć wielu jednocześnie otwartych zakładek.
4.21.3. Ewidencja otwieranych stron musi działać również, gdy otwierana jest strona z połączeniem szyfrowanym (https).
4.21.4. Ewidencja musi obejmować co najmniej: nazwę i adres IP komputera, nazwę użytkownika, datę i godzinę, adres strony, łączny czas korzystania, czas aktywności, czas pasywności.
4.21.5. W oparciu o algorytmy sztucznej inteligencji - machine learning oraz deep learning system umożliwia analizę treści rtcstron www oraz przypisanie im – w oparciu o treść – odpowiednich kategorii oraz kontrolowanie użytkowników pod kątem odwiedzanych stron.
4.21.6. Każda odwiedzona strona otrzymuje atrybuty: czy SSL, czy jest bezpieczna, czy zawiera przekierowania, czy znajduje się na liście CERT, czy znajduje się na liście stron hazardowych, czy kategoria strony jest bezpieczna, czy jest produktywna.
4.22. Monitorowanie serwerów WWW
4.22.1. System musi umożliwiać monitorowanie wybranych serwerów www.
4.22.2. System musi przedstawiać informację o działaniu wybranych serwerów oraz ich aktywności.
4.22.3. System musi posiadać możliwość weryfikacji treści (tekstu) dostępnego na monitorowanej stronie.

4.22.4. System w sposób graficzny musi przedstawiać działanie serwerów WWW wraz z wyszczególnieniem informacji dla każdego wybranego serwera (status, bieżący czas odpowiedzi, średni czas odpowiedzi za ostatnie 12 miesięcy, aktywność za ostatnie 3, 6, 12 miesięcy).

4.23. Monitorowanie dziennika zdarzeń

4.23.1. System musi posiadać możliwość monitorowania dziennika zdarzeń wszystkich komputerów.

4.23.2. Ewidencja zdarzeń musi następować w oparciu o definiowalną kategorię zdarzenia: critical, error, warning, info, audit failure, audit success, debug oraz typ dziennika: aplikacja, bezpieczeństwo, system.

4.23.3. System musi pozwalać na zdefiniowanie ewidencji zdarzeń z komputerów na podstawie kategorii zdarzenia.

4.23.4. Ewidencja musi zawierać: datę i godzinę zdarzenia, nazwę i adres IP komputera, typ zdarzenia, opis zdarzenia.

4.23.5. System musi umożliwiać monitorowanie komunikatów Syslog.

4.24. Monitorowanie pracy komputerów

4.24.1. System musi posiadać możliwość monitorowania daty włączenia i wyłączenia komputera niezależnie czy znajduje się w sieci lokalnej czy też poza nią i prezentować czas pracy komputera w układzie graficznym.

4.24.2. System musi posiadać ewidencję daty i godziny przyłączenia i odłączenia komputera od systemu monitorującego.

4.24.3. System musi ewidencjonować zdarzenia związane z logowaniem się użytkowników do danego komputera, również w przypadku podłączania się wielu użytkowników jednocześnie

4.25. Monitorowanie sesji zdalnych połączeń

4.25.1. System musi prowadzić ewidencję sesji zdalnych połączeń na każdym komputerze.

4.25.2. Informacja o nawiązanej sesji musi zawierać co najmniej: nazwę i adres IP komputera z którego nastąpiło połączenia, nazwę użytkownika nawiązującego połączenie, nazwę i adres IP komputera docelowego, adres portu połączenia.

4.26. Monitorowanie uprawnień ACL

4.26.1. System musi umożliwiać skanowanie list kontroli dostępu (ang., tzw. access-control list, ACL) z systemu katalogowego komputerów lokalnych oraz serwerów.

4.26.2. Dane muszą zawierać: nazwę komputera, ścieżkę, właściciela folderu, nazwę grupy uprawnień, listę nadanych uprawnień, datę aktualizacji.

4.26.3. Odczyt uprawnień na serwerach musi następować zgodnie ze zdefiniowanym harmonogramem.

4.26.4. System musi posiadać predefiniowane filtry pozwalające na filtrowanie uprawnień do zasobów lokalnych oraz współdzielonych.

4.26.5. Dane muszą być prezentowane w układach: Foldery -> Użytkownicy, Użytkownicy -> Foldery, Grupy -> Foldery, Właściciele -> Foldery.

4.26.6. System musi posiadać minimum trzy predefiniowane raporty prezentujące informacje zebrane podczas skanowania uprawnień.

4.27. Monitorowanie sensorów

4.27.1. System musi umożliwić integrację z systemem monitoringu warunków środowiskowych poprzez odczyt wartości z wykorzystaniem SNMP.

4.27.2. Czujniki muszą być grupowane wg typu oraz lokalizacji.

4.27.3. System musi prezentować położenie czujników na mapie wbudowanej w system.

4.27.4. System musi umożliwić odczyt informacji z czujników temperatury, wilgotności oraz odczytywać zmiany stanu czujników zalania oraz otwarcia drzwi.

4.27.5. System musi przechowywać odczytane dane w bazie danych przez zadany okres.

4.27.6. System musi umożliwić wysyłanie alertów poprzez email, sms oraz prezentować informację w konsoli o przekroczeniu monitorowanych parametrów.

4.27.7. System musi umożliwić graficzną prezentację danych zebranych z monitorowanych czujników.

4.28. Repozytorium CMDB – centralna baza systemu umożliwiająca import i eksport danych zarówno poprzez API jak też za pomocą wbudowanego import/eksporta, na którą składają się:

4.28.1. Active Directory - lista skonfigurowanych z konsolą serwerów LDAP, z których są importowane i aktualizowane dane o użytkownikach. System pozwala na wprowadzanie dowolnej ilości serwerów dla różnych domen.

4.28.2. Kontenery dokumentów - grupy, do których można przypisywać zapisane w systemie dokumenty w celu sortowania.

4.28.3. Kategorie aplikacji - lista kategorii, do których przynależą wykorzystywane przez użytkowników aplikacje.

4.28.4. Budżet - zestawienie typów budżetów (kosztów) zaewidencjonowanych w systemie.

4.28.5. Komputery - lista zinwentaryzowanych komputerów, podzielonych wg typu autoryzacji. Widok rekordu zawiera szczegółowe dane dotyczące danego komputera.

4.28.6. Dokumenty - repozytorium dokumentów zapisanych w systemie.

4.28.7. eLearning - zdefiniowane wiadomości typu eLearning. Wykorzystywane są do wysyłania użytkownikom szkoleń wbudowanych w system, zgodnie ze zdefiniowanym harmonogramem.

4.28.8. Kategorie plików - lista typów plików kategoryzowanych przez system. Administrator ma możliwość zdefiniowania własnych grup, do których pliki będą przydzielane, według wpisanej maski.

4.28.9. Pliki - lista zinwentaryzowanych plików ze wszystkich komputerów.

4.28.10. Licencje - zestawienie licencji zapisanych w bazie systemu, które administrator może przypisywać do poszczególnych użytkowników.

4.28.11. Typy licencji - lista typów licencji.

4.28.12. Lokalizacje - lista zdefiniowanych lokalizacji, do których administrator może przypisać poszczególnych użytkowników. W odróżnieniu od struktury organizacyjnej dane nie są importowane z Active Directory.

4.28.13. Typy urządzeń - lista typów urządzeń.

4.28.14. Urządzenia - lista urządzeń podzielonych wg typu.

4.28.15. Producenci / Dostawcy - lista producentów i dostawców.

4.28.16. Pamięć masowa - zestawienie dysków twardych z komputerów.

4.28.17. Porty sieciowe - lista monitorowanych portów sieciowych.

4.28.18. Usługi sieciowe - lista monitorowanych usług sieciowych.

4.28.19. Udostępnione zasoby sieciowe - lista udostępnionych zasobów sieciowych.

4.28.20. Sieci - lista definiowalnych ręcznie sieci, do których administrator może ręcznie przypisywać komputery.

4.28.21. Systemy operacyjne - zestawienie unikalnych systemów operacyjnych.

4.28.22. Struktura org. - zestawienie struktur organizacyjnych zdefiniowanych bądź importowanych z Active Directory.

4.28.23. Kategorie procesów - lista kategorii, do których będą przypisywane procesy aplikacji uruchamianych przez użytkowników. Klasyfikacja procesów odbywa się za pomocą algorytmów sztucznej inteligencji.

4.28.24. Serwery - lista zinwentaryzowanych serwerów.

4.28.25. Usługi - zestawienie usług działających na komputerach.

4.28.26. Oprogramowanie - lista zinwentaryzowanego i monitorowanego oprogramowania.

4.28.27. Uprawnienia ACL - lista uprawnień ACL jakie posiadają użytkownicy.

4.28.28. Pamięć masowa USB - lista urządzeń pamięci masowej USB.

4.28.29. Administratorzy - lista administratorów systemu,

4.28.30. Użytkownicy / pracownicy - lista pracowników.

4.28.31. Video LMS - lista filmów szkoleniowych dla pracowników.

4.28.32. Wirtualizacja » Maszyny - lista maszyn wirtualnych wraz z ich szczegółową specyfikacją.
4.28.33. Wirtualizacja » Serwery - lista serwerów wirtualizacji.
4.28.34. Kategorie WWW - lista kategorii stron WWW wykorzystywanych w procesie klasyfikacji stron internetowych. Klasyfikacja oparta o sztuczną inteligencję.
4.28.35. Serwisy WWW - lista monitorowanych serwisów WWW.
4.29. Worktime manager
4.29.1. System musi być wyposażony w zestaw statystycznych danych o pracy użytkownika i zdefiniowanych grup użytkowników.
4.29.2. Dane muszą być prezentowane w formie interaktywnych widgetów oraz w formie danych analitycznych.
4.29.3. Dane dla grup użytkowników muszą być skumulowane oraz analityczne.
4.29.4. Prezentacja danych odbywa się poprzez wskazanie pracownika lub grupy pracowników oraz wybranie okresu danych źródłowych.
4.29.5. Informacje dotyczące prezentowane w panelu to informacja o otwartych sesjach, informacja o sesjach historycznych, informacja o czasie zalogowania użytkownika, informacja o czasie pracy komputera, informacja o aktywności użytkownika w aplikacjach, informacja o produktywności użytkownika w aplikacjach, informacja o produktywności, wykorzystywanych aplikacjach, odwiedzonych stronach www z podziałem na kategorie stron, informacja o uruchomionych procesach z podziałem na kategorie, informacja o aktywności na stronach www, informacja o wykonanych wydrukach (nazwa dokumentu, data i godzina wydruku, drukarka, ilość stron, rodzaj wydruku – czarno-biały czy w kolorze, koszt wydruku), informacja o transferze sieciowym, informacja o zależności czasu pracy w trybach: zalogowany/ uśpiony/ wylogowany.
4.29.6. System musi umożliwić wyświetlanie informacji o użytkowniku pobranych z Active Directory. Informacje powinny być aktualizowane zgodnie z harmonogramem połączenia z domeną.
4.29.7. System musi prezentować w formie tabelarycznej informacje o dokumentach (np. protokoły przekazania i zwrotu sprzętu), komputerach i urządzeniach, które zostały przypisane użytkownikowi.
4.29.8. System musi posiadać widgety prezentujące dane w wybranym przedziale czasu: czas zalogowania – dni, czas pracy komputera – dni, aktywność w aplikacjach, produktywność w aplikacjach, produktywność w czasie pracy, czas pracy w aplikacjach, czas spędzony na stronach www wg kategorii stron, czas spędzony w aplikacjach (procesach) wg kategorii procesu, czas aktywność na stronach www, stron wydruku wg dokumentów, transfer sieciowy, czas pracy wg zalogowany/ wylogowany / uśpiony, czas aktywności w godzinach pracy.
4.30. Raportowanie i eksport danych
4.30.1. Systemu musi umożliwiać wyeksportowania wybranych lub wszystkich danych do formatu xls, csv, OpenOffice calc, html, mht, xml, jpeg, png, gif, bmp.
4.30.2. System musi mieć możliwość kategoryzowania raportów (spośród wszystkich raportów) oraz dodawania raportów użytkownika (zaprojektowanych przez użytkownika).
4.30.3. System musi umożliwiać generowanie raportów bezpośrednio z każdego widoku w aplikacji z zastosowaniem bieżących filtrów.
4.30.4. Generowanie raportu musi odbywać się po stronie serwera a nie klienta.
4.30.5. System musi umożliwiać wieloinstancyjność raportowania (wiele otwartych raportów jednocześnie z wielu widoków).
4.30.6. System musi mieć możliwość generowania i wyświetlania dowolnych wieloparametrycznych raportów w standardzie SAP Crystal Reports (rpt).
4.30.7. System musi umożliwiać eksport danych z raportu do formatów: RPT, PDF, XLS, DOC, RTF.
4.30.8. System musi obsługiwać raporty parametryczne z parametrami statycznymi (wprowadzanymi w momencie generowania raportów) oraz dynamicznymi (pobieranymi z bazy danych w momencie generowania raportu).

4.30.9. System musi posiadać co najmniej 150 zdefiniowanych raportów dotyczących wszystkich obszarów funkcjonalnych.

4.30.9.1. Raporty z zakresu komputerów

- Komputery – Karta graficzna – Procesor
- Komputery – Serwery wg systemu operacyjnego
- Komputery wg procesora – Skrócony
- Komputery wg procesora – Wszystkie
- Komputery wg producenta – Skrócony
- Komputery wg producenta – Wszyscy
- Komputery wg struktur organizacyjnych – Skrócony
- Komputery wg struktury organizacyjnej – Wszystkie
- Komputery wg systemów operacyjnych – Skrócony
- Komputery wg systemów operacyjnych – Wszystkie
- Komputery wg typu – Desktop
- Komputery wg typu – Hyper-V
- Komputery wg typu – Mobile
- Komputery wg typu – Nieokreślone
- Komputery wg typu – Server
- Komputery wg typu – Virtual Machine
- Komputery wg typu – VMWare
- Komputery wg typu – Wszystkie typy
- Zestawienie komputerów wg typu – Skrócony
- Komputery online
- Komputery niezautoryzowane
- Komputery offline
- Komputery online
- Komputery w magazynie
- Komputery w naprawie
- Komputery wszystkie
- Komputery wycofane
- Komputery zablokowane
- Komputery zautoryzowane
- Komputery zlikwidowane
- Komputery z Intel Anti-Theft
- Komputery z Intel VPro

4.30.9.2. Raporty z zakresu wirtualizacji

- Wirtualizacja – Maszyny wirtualne
- Wirtualizacja – Serwery wirtualizacji
- Wirtualizacja

4.30.9.3. Raporty z zakresu urządzeń

- Urządzenia – Notatki
- Urządzenia – USB – Dodane
- Urządzenia – USB – Wykryte
- Urządzenia – USB – Wszystkie
- Urządzenia – USB – Biała lista
- Urządzenia – Serwis
- Urządzenia – Inwentaryzacja – Kody kreskowe
- Urządzenia – Inwentaryzacja

- Urządzenia – Inwentaryzacja – Porównanie inwentaryzacji
- Urządzenia – Utrzymanie
- Urządzenia

4.30.9.4. Raporty z zakresu sieci

- Sieć – Wykryte
- Sieć – Historia
- Sieć – Ostanie skanowanie

4.30.9.5. Raporty z zakresu oprogramowania

- Oprogramowanie – Systemy operacyjne – Wszystkie
- Oprogramowanie – Systemy operacyjne – Instalacje OEM
- Oprogramowanie – Systemy operacyjne – Szczegóły
- Oprogramowanie – Systemy operacyjne – Historia audytów
- Oprogramowanie – Aplikacje – Wszystkie
- Oprogramowanie – Aplikacje – Monitorowane
- Oprogramowanie – Aplikacje – Szczegóły
- Oprogramowanie – Aplikacje – Historia audytów
- Oprogramowanie – Pakiety – Wszystkie
- Oprogramowanie – Pakiety – Szczegóły
- Oprogramowanie – Pakiety – Historia audytów
- Oprogramowanie – Bazy danych – Wszystkie
- Oprogramowanie – Bazy danych – Express
- Oprogramowanie – Bazy danych – Pozostałe
- Oprogramowanie – Bazy danych – per Core
- Oprogramowanie – Rejestry – Razem
- Oprogramowanie – Rejestry – Szczegóły
- Oprogramowanie – Rejestry – Ostatnio zainstalowane
- Oprogramowanie – Klucze produktu
- Oprogramowanie – Wykorzystanie – Użycie – Wszystkie
- Oprogramowanie – Wykorzystanie – Oszczędności
- Oprogramowanie – Wykorzystanie – CAL
- Oprogramowanie – Wykorzystanie – CAL WEB
- Oprogramowanie – Monitorowanie – Uruchomienia
- Oprogramowanie – Monitorowanie – Aktywność ogółem

4.30.9.6. Raporty z zakresu osób

- Osoby – Protokół standardowy
- Osoby – Protokół rozszerzony

4.30.9.7. Raporty z zakresu plików i multimediów

- Pliki i multimedia – Archiwa
- Pliki i multimedia – Audio
- Pliki i multimedia – Erotyka
- Pliki i multimedia – Grafika
- Pliki i multimedia – Wideo
- Pliki i multimedia – Wykonywalne
- Pliki i multimedia – Zmiany plików

4.30.9.8. Raporty z zakresu magazynu

- Magazyn – Dokumenty
- Magazyn – Stany
- Magazyn – Materiały

- Magazyn

4.30.9.9. Raporty z zakresu finansów

- Finanse – Urządzenia
- Finanse – Licencje
- Finanse – Wydruki wg drukarki
- Finanse – Wydruki wg sterownika
- Finanse – Wydruki użytkownicy
- Finanse – Magazyn

4.30.9.10. Raporty z zakresu serwera wiadomości

- Serwer wiadomości – Komunikator – Historia
- Wiadomość cykliczna – wg wiadomości
- Serwer wiadomości – Komunikator – Rozmowy
- Serwer wiadomości – Wiadomości wysłane – wg komputera
- Serwer wiadomości – Wiadomości wysłane – wg odbiorcy
- Serwer wiadomości – Wiadomości wysłane – wg wiadomości
- Serwer wiadomości – Wiadomości wysłane – wg wysyłającego
- Serwer wiadomości – Wiadomości – Aktywne cykle

4.30.9.11. Raporty z zakresu serwera wideo (LMS)

- Serwer wideo (LMS) – Proces szkoleniowy – Filmy
- Serwer wideo (LMS) – Proces szkoleniowy – Filmy – Zakończone
- Serwer wideo (LMS) – Proces szkoleniowy – Schematy
- Serwer wideo (LMS) – Proces szkoleniowy – Schematy – Zakończone
- Serwer wideo (LMS) – Certyfikaty
- Serwer wideo (LMS) – Pracownicy

4.30.9.12. Raporty z zakresu serwera monitorującego

- Serwer monitorujący – Logowanie agentów
- Serwer monitorujący – eServer
- Serwer monitorujący – Alerty systemowe
- Serwer monitorujący – Historia logowań
- Serwer monitorujący – Dzienniki zdarzeń – Powiadomienia systemowe
- Serwer monitorujący – Dzienniki zdarzeń – Dzienniki
- Serwer monitorujący – Dzienniki zdarzeń – Sesje RDP
- Serwer monitorujący – Transfer sieciowy – Procesy
- Serwer monitorujący – Drukowanie
- Serwer monitorujący – Drukowanie – Razem
- Serwer monitorujący – Drukowanie – Razem SNMP
- Serwer monitorujący – Drukowanie – Prognoza
- Serwer monitorujący – Usługi – Wszystkie
- Serwer monitorujący – Usługi – Szczegóły
- Serwer monitorujący – Harmonogram zadań
- Serwer monitorujący – Sesje VNC
- Serwer monitorujący – Intel AMT
- Serwer monitorujący – Poczta wychodząca
- Serwer monitorujący – Strony www – Odwiedzone
- Serwer monitorujący – Strony www – Aktywność ogółem
- Serwer monitorujący – USB
- Serwer monitorujący – Wydajność – CPU
- Serwer monitorujący – Wydajność – Dysk

- Serwer monitorujący – Wydajność – Dysk (razem)
- Serwer monitorujący – Wydajność – Pamięć
- Serwer monitorujący – Wydajność – Procesy
- Serwer monitorujący – Wydajność – Sieć

4.30.9.13. Raporty z zakresu serwera zadań
- Serwer zadań – Logi
- Serwer zadań – Zadania cykliczne

4.30.9.14. Raporty z zakresu serwera automatyzacji
- Serwer automatyzacji – Automaty
- Serwer automatyzacji – Logi

4.30.9.15. Raporty z zakresu raportów
- Raporty – Harmonogram
- Raporty – Harmonogram – Historia

4.30.9.16. Raporty z zakresu repozytorium
- Repozytorium – Dokumenty
- Repozytorium – e-Learning
- Repozytorium – Kategorie aplikacji
- Repozytorium – Kategorie plików
- Repozytorium – Kategorie procesów
- Repozytorium – Kategorie www
- Repozytorium – Producenci Dostawcy
- Repozytorium – Typy licencji
- Repozytorium – Zdalna instalacja – Repozytorium
- Repozytorium – Zdalna instalacja – Logi

4.30.9.17. Raporty z zakresu ustawień
- Ustawienia – Administratorzy – Wszystkie
- Ustawienia – Dane firmy
- Ustawienia – Struktura organizacyjna
- Ustawienia – Budżet
- Ustawienia – Sieci

4.30.10. System musi posiadać możliwość ustalenia harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu.

4.30.10.1. Wynikiem wykonania harmonogramu jest raport w formacie pdf.

4.30.10.2. Harmonogram można skonfigurować.

4.31. Powiadomienia

4.31.1. System musi umożliwiać generowanie powiadomienia w formie alertu w konsoli systemu, wiadomości email wysłanej na wybrane adresy oraz wiadomości SMS na wskazane numery telefonów.

4.31.2. System musi umożliwiać tworzenie wybranych powiadomień wiele razy z określeniem innych grup obiorców

4.31.3. System musi umożliwiać edycję treści wysyłanych powiadomień i możliwość korzystania z danych umieszczonych w systemie w treści powiadomienia.

4.31.4. System musi posiadać co najmniej 30 zdefiniowanych powiadomień dotyczących obszarów funkcjonalnych

4.31.5. Powiadomienia z zakresu oprogramowania
- Odinstalowano oprogramowanie
- Wykryto niezgodność ze schematem oprogramowania
- Wykryto nowe oprogramowanie

4.31.6. Powiadomienia z zakresu sieci
- Monitorowana usługa sieciowa przestała odpowiadać
- Monitorowane urządzenia z problemami
- Monitorowane urządzenie jest offline
- Problem ze stroną WWW
- Serwis WWW nie odpowiada
- Serwis WWW odpowiada niewłaściwym komunikatem
- Średni czas odpowiedzi usługi przekroczył wartość X ms
- Transfer sieciowy na komputerze przekroczył X MB / Y min
- W sieci pojawiły się duplikaty adresów IP
- W sieci pojawiły się duplikaty adresów MAC
- Wykryto dużą ilość danych wysyłanych przez dany port w switch'u
- Wykryto nowe urządzenie
- Wykryto urządzenie z odblokowanym portem X
- Wykryto urządzenie z usługą X
- Wykryto zmianę adres IP komputera
- Wykryto zmianę statusów portów w switch'u

4.31.7. Powiadomienia z zakresu sprzętu
- Interfejs sieciowy wyłączony
- Parametr lub parametry S.M.A.R.T. przekroczyły dozwolone wartości
- Podłączono urządzenie USB
- Wykryto zmianę w sprzęcie (WMI)

4.31.8. Powiadomienia z zakresu systemu
- Mało miejsca na dysku C
- Pojawił się błąd w dzienniku zdarzeń Windows
- Wykryto problem z usługą systemu Windows
- Wykryto zmianę nazwy komputera
- Wysokie użycie pamięci RAM
- Zmieniono informację o systemie

4.31.9. Powiadomienia z zakresu użytkownika
- Użytkownik odwiedził stronę WWW z wybranej kategorii
- Użytkownik przekroczył limit wydrukowanych stron
- Użytkownik przekroczył transfer sieciowy X MB / Y min

5. Bezpieczeństwo

5.1. System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.

5.2. Uwierzytelnianie do systemu musi być realizowane:

5.2.1. z wykorzystaniem imiennego konta użytkownika i hasła,

5.2.2. z wykorzystaniem imiennego konta administratorów aplikacji i hasła,

5.2.3. za pośrednictwem jednokrotnego uwierzytelniania poprzez Active Directory,

5.2.4. za pośrednictwem jednokrotnego uwierzytelniania poprzez CAS,

5.2.5. za pomocą kluczy uwierzytelniających.

5.3. Hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej.

5.4. Siła hasła musi być definiowalna w zakresie atrybutów: ilość znaków, ilość liter, ilość znaków specjalnych, ilość małych znaków, ilość wielkich znaków, ilość cyfr, ilość znaków specjalnych, ilość znaków alfanumerycznych, lista dopuszczalnych znaków specjalnych, lista wyłączonych znaków).

5.5. Prawa dostępu muszą opierać się na grupach i użytkownikach w zakresie: przeglądanie / edycja / usuwanie/ eksport.

5.6. System musi umożliwiać zastosowanie dodatkowej autentykacji podczas logowania przy użyciu certyfikatu SSL w systemie lub na tokenie.
5.7. Uwierzytelnianie za pomocą kluczy
5.7.1. Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe wraz z hasłem, które umożliwia jednoczesną pracę wielu użytkownikom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory/LDAP.
5.7.2. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania w oparciu o RSA 512/1024/RSA 2048 bit, ECDSA 192/256 bit, DES/3DES, AES 128/192/256 bit, SHA-1 / SHA-256.
5.7.3. Wykorzystywane klucze muszą posiadać wsparcie dla systemów Windows 7/8.1/10 i Windows Server 2012/2016/2019.
5.8. System musi udostępniać historię korzystania z poszczególnych opcji przez wybranych użytkowników/administratorów.
5.9. System musi posiadać wbudowany mechanizm automatycznej synchronizacji czasu pomiędzy agentami oraz serwerem, gdzie wzorcowy czas jest po stronie serwera.
5.10. System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nieprzyrostowej oraz udostępniać informacje o rezultacie wykonania kopii.
5.11. System musi pobierać dane z widoków (view) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych.
5.12. W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, agenci, serwer, baza danych, bazy wiedzy).
5.13. System musi być wyposażony w mechanizmy powtórnego załadowania danych historycznych pochodzących od agentów.
5.14. System musi zapewniać:
5.14.1. Pełne logowanie błędów w celu weryfikowania nieprawidłowości.
5.14.2. Przechowywanie logów systemowych.
5.14.3. Przechowywanie logów bezpieczeństwa.
5.14.4. Przechowywanie logów aktywności użytkowników i administratorów.
5.14.5. Pobieranie logów z agentów z poziomu konsoli administracyjnej.
5.14.6. Możliwość eksportu logów.
5.14.7. Definiowanie maksymalnego czasu przechowywania plików log.
5.15. System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.
6. Wsparcie i pomoc
6.1. System musi posiadać dokumentację w postaci min. 20 filmów instruktażowych/nagrań z webinarów w języku polskim.
6.2. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim.
6.3. Pomoc techniczna musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.

POZ. 2 – Przełącznik - dedykowane urządzenie sieciowe

	Minimalne wymaganie dotyczące jednej sztuki przełącznika CORE 10G.
1.	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2.	Wymagane parametry fizyczne: a) możliwość montażu w stelażu/szafie 19”

	b) wysokość maksymalna 1U c) Możliwość instalacji dwóch wewnętrzne redundantne zasilacze 230V AC typu hot-swap (nie dopuszcza się rozwiązania zewnętrznego). Każde urządzenie musi zostać dostarczone z minimum 2 zasilaczem umożliwiające wymianę w trakcie pracy urządzenia (ang. hot-swap). d) zakres temperatur pracy ciągłej co najmniej od -5 do +45 °C e) zakres wilgotności pracy co najmniej 10% - 95% f) port USB umożliwiający podłączenie zewnętrznej pamięci flash
3.	Urządzenie musi być wyposażone w 4 wentylatory z możliwością wymiany pojedynczego wentylatora lub całego modułu wentylatorów w trakcie pracy urządzenia (ang. hot-swap).
4.	Przełącznik musi zostać dostarczony z następującymi interfejsami mogącymi działać równocześnie: ● 24 portów 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 10G-ER, 1G-LX, 1G-SX ● 6 portów 40G QSFP+ z obsługą modułów 40G-SR, 40G-LR Wszystkie porty muszą być dostępne od frontu urządzenia. Urządzenie musi umożliwiać w przyszłości zwiększenie przepustowości portów 40G do prędkości 100G poprzez zakup dodatkowej licencji bądź możliwość instalacji dodatkowego modułu z 6 portami 100G. W ramach postępowania Zamawiający nie wymaga dostarczenia takiej licencji bądź dodatkowego modułu z 6 portami 100G. Zamawiający nie dopuszcza aby realizacja portów 10G była realizowana poprzez tzw. rozszywanie portów 10G/40G na 4 porty 10G. Wszystkie interfejsy 10G, 40G/100G muszą być dostępne z przodu obudowy.
5.	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: a) Zarządzanie stosem poprzez jeden adres IP b) Do min. 4 jednostek w stosie c) Magistrala stackująca o wydajności 1.35 Tbit/s d) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation) e) Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree f) Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia. Zamawiający dopuszcza aby możliwość łączenia w stosy była realizowana za pomocą portów typu uplink.
6.	Układ przełączający o wydajności min. 1,68 Tbps
7.	Obsługa min. 300 000 adresów MAC
8.	Wbudowana pamięć RAM min. 4 GB Procesor wielordzeniowy.
9.	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 2 GB
10.	Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
11.	Możliwość skonfigurowania min. 1000 interfejsów vlan interface SVI działających równocześnie.
12.	Obsługa standardów IEEE: - CFM zgodny z 802.1ag - EFM zgodny z 802.3ah
13.	Obsługa ramek jumbo o wielkości min. 9216 bajtów
14.	Obsługa protokołu GVRP lub VTP
15.	Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP.
16.	Obsługa min. 256 000 tras dla routingu IPv4
17.	Obsługa min. 80 000 tras dla routingu Ipv6
18.	Obsługa protokołów routingu OSPF, OSPFv3, IS-IS, IS-Isv6, BGPv4, BGPv4+, RIP, RIPng, PIM-SM,

	PIM-DM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania. Dla protokołów BGP, IS-IS oraz OSPF obsługa protokołu BFD.
19.	Obsługa VRF
20.	Obsługa protokołów LLDP i LLDP-MED.
21.	Wsparcie dla technologii MPLS, w tym L3 VPN. Jeżeli funkcjonalność MPLS wymaga licencji to należy ją dostarczyć w ramach niniejszego postępowania
22.	Przełącznik musi posiadać funkcjonalność DHCP Server
23.	Obsługa ruchu multicast: ● IGMP v1, v2 i v3 ● IGMP Snooping v1, v2 I v3
24.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: a) min. 4 poziomy dostępu administracyjnego poprzez konsolę b) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL c) możliwość utworzenia minimum 5000 list ACL d) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www e) zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów Ipv4 i Ipv6 f) możliwość filtrowania ruchu w oparciu o adresy MAC, Ipv4, Ipv6, porty TCP/UDP g) obsługa mechanizmów Dynamic ARP, , voice VLAN oraz private VLAN (lub równoważny), h) możliwość synchronizacji czasu zgodnie z NTP i) wsparcie dla RMON, RMON2 j) wsparcie dla protokołu NETCONF
25.	Obsługa funkcjonalności UDLD lub równoważnej
26.	Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach: ● klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP ● wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR
27.	Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA). Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania.
28.	Wymagane opcje zarządzania: a) możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN b) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC) c) dedykowany port konsoli, zgodny ze standardem RS-232 d) dedykowany port zarządzający out-of-band Ethernet 10/100Base-T
29.	Wraz z urządzeniami muszą zostać dostarczone: a) pełna dokumentacja w języku polskim lub angielskim b) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana

30.	Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
31.	Wsparcie dla funkcjonalności VXLAN L2 i L3. Jeżeli obsługa powyżej funkcjonalności wymaga dodatkowej licencji to w ramach niniejszego postępowania Zamawiający nie wymaga jej dostarczenia.
32.	Przełącznik musi mieć możliwość pracy jako kontroler WLAN poprzez instalację dodatkowej licencji bądź modułu rozszerzeń instalowanego w obudowie urządzenia. Możliwość obsługi minimum 200 punktów dostępowych. Jeżeli funkcjonalność kontrolera WLAN wymaga dodatkowej licencji bądź modułu to w ramach niniejszego postępowania Zamawiający nie wymaga ich dostarczenia.
33.	Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski
34.	Zamawiający wymaga, aby przełącznik posiadał 3-letni serwis gwarancyjny, świadczony przez Wykonawcę na bazie wsparcia serwisowego producenta. Wsparcie serwisowe na dostarczone urządzenia musi być zarejestrowane u producenta na Zamawiającego. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego zarejestrowanie/nabycie serwisu gwarancyjnego na Zamawiającego.
35.	Przełącznik CORE musi pochodzić od tego samego producenta co oferowane przełączniki dostępowe w celu zapewnienia spójnego zarządzania oraz pełnej kompatybilności pomiędzy urządzeniami
36.	Urządzenie musi posiadać gwarancję producenta typu Limited Lifetime Warranty.
37.	Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzeń

POZ. 3 – Macierz

Nazwa komponentu	Wymagane minimalne parametry techniczne pojedynczej macierzy
Obudowa	Urządzenie musi być przeznaczone do instalacji w szafie technicznej typu RACK 19”, dostarczone ze wszystkimi niezbędnymi komponentami do montażu.
Kontrolery dyskowe	Minimum dwa kontrolery pracujące w trybie Symmetrical Active-Active (SAN-only), to znaczy w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów w trybie bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing). Kontrolery muszą pozwalać na udostępnianie zasobów protokołem FC, iSCSI w zależności od zastosowanych kart komunikacyjnych. Komunikacja pomiędzy parą kontrolerów (synchronizacja cache) macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem urządzeń aktywnych FC/Ethernet/Infiniband. Zamawiający dopuszcza komunikację z wykorzystaniem urządzeń aktywnych przy klastrze wielu kontrolerów. Każdy z kontrolerów musi mieć możliwość

	jednoczesnej prezentacji (aktywny dostęp odczyt i zapis) wszystkich wolumenów utworzonych w logicznych ramach całego systemu dyskowego. Kontrolery muszą być wyposażone w procesory o sumarycznej ilości min. 48 rdzeni (ang.: core)
Możliwość rozbudowy	Macierz umożliwia rozbudowę do 6 par kontrolerów dyskowych tworzących jedna logiczną macierz, bez konieczności wymiany zaoferowanej pary kontrolerów. Za jedną logiczną macierz uznaje się rozwiązanie, w którym zarządzanie wszystkimi kontrolerami jest możliwe z jednego interfejsu GUI, CLI. Nie dopuszcza się rozwiązanie oparte o wirtualizator. Macierz musi umożliwiać rozbudowę do co najmniej 70 sztuk oferowanego typu modułów pamięci, bez wymiany kontrolerów macierzowych oraz bez potrzeby zakupu dodatkowych licencji. (tylko poprzez dodawanie półek i modułów NVMe oraz przełączników, jeśli rozbudowa o dużą liczbę półek tego wymaga). Półki dyskowe muszą być podłączane poprzez porty o przepustowości min. 50Gb/s z obsługą protokołu RDMA.
Wymagana przestrzeń	Macierz musi być skonstruowana wyłącznie do obsługi modułów pamięci NVMe i w żadnej konfiguracji nie może obsługiwać przestrzeni danych użytkownika na dyskach obrotowych/talerzowych. Moduły pamięci NVMe muszą być wyposażone w podwójne, redundantne interfejsy PCIe. Min 10 dysków NVMe o pojemności 3.84TB.
Pamięć Cache	Urządzenie zbudowane z dwóch kontrolerów musi być wyposażone w co najmniej 192 GB pamięci podręcznej cache obsługującej operacje odczytu i zapisu zbudowane w oparciu o wydajną pamięć RAM. Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin.
Zabezpieczenie danych	Urządzenie musi obsługiwać poziomy RAID5 i RAID6 (RAID z dystrybuowaną przestrzenią zapasową typu hot-spare) lub równoważne poziomy RAID zabezpieczające przed awarią dwóch dysków jednocześnie. Macierz musi umożliwiać również skonfigurowanie poziomu RAID zapewniającego odporność na jednoczesną awarię 3 dysków. Możliwość definiowania dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.
Dostępne interfejsy	Każdy kontroler udostępnia minimum: Porty front-end: • 8 interfejsów 10Gb Eth SFP+ Porty back-end: • 2 porty SAS 12Gb/s Macierz umożliwia rozbudowę każdego kontrolera o dodatkowe interfejsy minimum: 8 portów FC 32Gb/s obsługujących protokół NVMe over Fibre Channel w ramach zaoferowanej ilości kontrolerów oraz możliwość podłączania serwerów bezpośrednio do tych portów macierzy bez użycia przełączników. Wszystkie porty muszą być obsadzone odpowiednimi modułami SFP+. Macierz musi być wyposażone w komplet okablowania w tym kable zasilające i

	światłowody o długości 3m.
Brak pojedynczego punktu awarii	Wszystkie krytyczne komponenty takie jak adaptery HBA, kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo: tak, aby awaria pojedynczego elementu nie wpływała na ciągłość dostępu do danych całego systemu. Komponenty te muszą być wymienialne w trakcie pracy.
Prezentacja dysków logicznych o pojemności większej niż zajmowana przestrzeń dyskowa (Thin Provisioning)	Wymagana jest funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
Snapshoty	Urządzenie musi umożliwiać utworzenie 800 kopii migawkowych (ang. snapshot) w trybie ROW (ang. Redirect on Write) dla pojedynczego wolumenu oraz minimum 5000 dla całej macierzy. Niedopuszczalne jest wykonywanie kopii w technologii COW (ang. Copy-on-Write). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. Rozwiązanie musi umożliwiać hierarchiczne tworzenie kopii migawkowych (np. kopia z kopii z kopii).
Wydajność	Wydajność średnia uzyskiwana w oferowanej konfiguracji nie mniejsza niż **90 000 IOPS** (ilość operacji na sekundę) dla obciążenia uzyskiwanego bezpośrednio z podsystemu dysków, bez deduplikacji i kompresji (0% trafień w cache do odczytu oraz zapisu), odczyt/zapis 100% losowy, protokołu FC i charakterystyki obciążenia dla bloków 8KB w proporcjach odczyt 60%, zapis 40% i czas odpowiedzi na poziomie 1 ms lub mniej. Środowisko testowe – serwery wirtualne udostępnione na VMware ESXi poprzez protokół FC. Wykonawca jest zobowiązany do wykazania wydajności przez przedstawienia oświadczenia producenta o spełnieniu wymagania lub wydruku raportu z oprogramowania do projektowania i skalowania rozwiązań pamięci masowej producenta (tzw. sizer'a) potwierdzającego spełnienie powyższych wymagań.
Funkcje kopiujące	Tworzenie na żądanie pełnej kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z woluminu źródłowego na docelowy oraz resynchronizację danych z woluminu docelowego na źródłowy np. w sytuacji uszkodzenia danych na woluminie źródłowym. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
Redukcja danych	Macierz musi mieć możliwość włączenia funkcjonalności deduplikacji i kompresji danych w trybie in-line, a ponadto musi ona umożliwiać: • włączenie deduplikacji dla poszczególnych wolumenów, • wyłączenie deduplikacji dla poszczególnych wolumenów na których wcześniej deduplikacja była włączona, • włączenie kompresji dla poszczególnych wolumenów, • wyłączenie kompresji dla poszczególnych wolumenów na których wcześniej kompresja była włączona, • uruchomienia jednocześnie deduplikacji i kompresji dla dowolnego wolumenu, Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

Replikacja danych	Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym - po protokołach FC lub iSCSI bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji, główek typu serwer/wirtualizator, itp. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
Klaster wysokiej dostępności	Model oferowanej macierzy musi wspierać rozwiązanie klastra „wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów danych macierzy dla podłączonych platform software'owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po FC lub iSCSI pomiędzy minimum 2 macierzami. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności", musi wspierać klastrownie wybranych woluminów bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną. Musi być możliwość dodawania woluminów objętych zabezpieczeniem w klastrze bez konieczności zatrzymywania replikacji. Funkcjonalność „wysokiej dostępności" musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover). Funkcjonalność „wysokiej dostępności" musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover). Funkcjonalność „wysokiej dostępności" musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback). Funkcjonalność „wysokiej dostępności" musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
Priorytety zadań	Macierz musi posiadać funkcjonalność zarządzania wydajnością, która dynamicznie przydziela zasoby macierzy w celu spełnienia określonych celów wydajnościowych aplikacji (QoS). Możliwość ustawiania priorytetów wydajności dla aplikacji w oparciu o zdefiniowane profile wolumenowe, dla wydajności w IOPS i przepustowości danych. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
Kompatybilność	Model oferowanej macierzy musi znajdować się na oficjalnej liście zgodności VMware (dostępnej na stronie https://www.vmware.com/resources/compatibility/search.php) dla kryterium wyszukiwania "Site Recovery Manager (SRM) for SRA" i produktu "SRM 8.3" lub jego nowszej dostępnej aktualizacji.
Wielościeżkowość	Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy

	kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: Windows Server 2016/2019, Vmware 6.7 i 7.0, CentOS.
Zasilanie	Urządzenie musi cechować wsparcie dla zasilania z dwóch niezależnych źródeł prądu jednofazowego o napięciu 200-240V i częstotliwości 50-60Hz poprzez nadmiarowe zasilacze typu Hot-Swap.
Zarządzanie macierzą	Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności modułów NVME. Konsola graficzna musi być dostępna poprzez przeglądarkę internetową i być elementem systemu operacyjnego macierzy. Wymaga możliwość dostępu do danych wydajnościowych historycznych z poziomu GUI co najmniej 1 rok wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożlwiającym zbieranie i przeglądanie danych historycznych. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
Serwisowalność	Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych. Macierz musi umożliwiać zdalne zarządzanie oraz automatyczne informowanie centrum serwisowego o awarii. Zgłoszenia usterek muszą być akceptowane zarówno drogą email jak również drogą telefoniczną.
Gwarancja, wsparcie serwisowe	Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP. Macierz dyskowa musi zostać objęta minimum 5 letnim okresem gwarancji w trybie onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta. Usługi gwarancyjne świadczone przez wykonawcę/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001:2008 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001:2008 lub równoważny. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków: • bezpłatna możliwość aktualizacje firmware; • dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń; • dostęp do centrum pomocy technicznej producenta; • otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware; • otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy

POZ. 4 – System ochrony poczty

Wymagania ogólne

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systemu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Parametry fizyczne systemu antyspamowego

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.

15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.
10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.

Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.

13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)
17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Ochrona przed atakami na usługę poczty

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

Aktualizacje sygnatur, dostęp do bazy spamu

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

Certyfikaty

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

Serwisy i licencje

System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 36 miesięcy.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

POZ. 5 – Szkolenie

W ramach przedmiotu zamówienia Wykonawca zapewni szkolenie w formie stacjonarnej lub online, dla minimum 15 osób w zakresie: Zarządzanie ryzykiem, dokumentacją i polityką bezpieczeństwa w jednostkach publicznych w świetle rozporządzenia Rady Ministrów z dn. 12.04.2012r.

Szkolenie musi zawierać min.:

1. Krajowe Ramy Interoperacyjności (KRI) – ustawa o informatzacji podmiotów publicznych realizujących zadania publiczne oraz rozporządzenie KRI
2. Ustawa o krajowym systemie cyberbezpieczeństwa (KSC)

3. Przepisy o ochronie danych osobowych - RODO i UODO
4. Procesy zarządzania bezpieczeństwem informacji
5. Odpowiedzialność za bezpieczeństwo informacji w podmiocie realizującym zadanie publiczne;
6. Zarządzanie ryzykiem w KRI:
a) Identyfikacja aktywów chronionych, w tym danych osobowych;
b) Klasyfikacja aktywów, w tym systemów kluczowych;
c) Metoda identyfikacji ryzyka;
d) Metoda analizy ryzyka;
e) Zasady oceny ryzyka;
7. Zarządzanie incydentami KRI i RODO;
a) Definicja incydentu;
b) Kryteria incydentów KRI;
c) Zintegrowane zasady obsługi incydentów;
d) Zasady zgłaszania incydentów.

I zakończyć się zaświadczeniem potwierdzającym odbycie szkolenia.