**CZĘŚĆ A**

1. **Listwy zasilające Rack – 10 szt.**
	1. Standard RACK 19"
	2. Wysokość 1 U
	3. Ilość gniazd 8 z uziemieniem typu E
	4. Wtyczka typu E
	5. Włącznik sieciowy Tak - podświetlany
	6. Długość przewodu zasilającego – nie krótsza niż 2 m
	7. Grubość kabla zasilającego – co najmniej 1,5mm²
	8. Maksymalne obciążenie – nie mniejsze, niż 3680 W
2. **Przełącznik sieciowy zarządzalny (switch) – 17 szt.**
	1. nie mniej niż 8 portów Ethernetowych 10/100/1000 Mbps
	2. przepustowość 20 Gbps
	3. Obsługa anomalii nadawczych (broadcast storm control),
	4. Obsługa wielu VLANs,
	5. Obsługa STP,
	6. Obsługa agregacji linków ( IEEE 802.3ad ) po minimum 8 grup na agregacje linku
	7. Funkcja izolacji portu w celu zwiększenia bezpieczeństwa portów,
	8. Obsługa IGMP snooping v1, v2, v3,
	9. Obsługa rejestracji multicastu VLAN,
	10. Obsługa zaawansowanych funkcje bezpieczeństwa, takie jak ACL, dynamiczna inspekcja ARP i więcej,
	11. Obsługa zarządzania switchem SNMP v1, v2c oraz v3,
	12. Obsługa zarządzania switchem poprzez SSH v1/v2.
	13. Zarządzalny – co najmniej L2
	14. Minimalna ilość portów SFP - X2, LAN - 1GB X8
	15. Typ obudowy Rack 19"
	16. Standardy przewodowe IEE 802.3 10Base-T, IEE 802.3u 100Base-TX, IEE 802.3ab 1000Base-T, IEEE 802.3z 1000Base-LX/SX, IEEE 802.3x, IEEE 802.3ad, IEEE 802.1p, IEEE 802.1q, IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, IEEE 802.1x, IEEE 802.ad LACP, IEEE 802.1d (Classic STP), IEEE 802.1w (Rapid STP), IEEE 802.1s (Multiple STP), IEEE 802.1q (Tag-based VLAN), IEEE 802.1x (Port-Based/MAC-Based Authentication), RADIUS/TACACS, ACL (Access Control List), IGMP Snooping V1/V2/V3, LLDP (Link Layer Discovery Protocol), DLDP (Device Link Detection Protocol)
	17. Przepustowość co najmniej 20 Gbps
	18. Tablica adresów MAC conajmniej 8 k
	19. Bufor nie mniejszy niż 4.1 Mbit
	20. Zarządzanie Web, SNMP v1/v2c/v3, SSH v1/v2
	21. Chłodzenie Pasywne
	22. Uchwyty do montażu w szafie Rack w komplecie
3. **Przełącznik sieciowy zarządzalny (switch) – 3 szt.**
	1. Nie mniej niż 24 porty 10/100/1000 RJ-45 z automatycznym wykrywaniem szybkości (10BASE-T typu IEEE 802.3, 100BASE-TX typu IEEE 802.3u, 1000BASE-T typu IEEE 802.3ab),
	2. Dupleks: 10BASE-T/100BASE-TX: pełny dupleks lub półdupleks 1000BASE-T: pełny dupleks
	3. Nie mniej niż 4 porty SFP typu dual personality z automatycznym wykrywaniem szybkości
	4. Co najmniej 2 gniazda modułu rozszerzenia portu
	5. Co najmniej 1 port szeregowy konsoli RJ-45
	6. Nie mniej niż 128 MB SDRAM, pojemność bufora pakietów 2MB, 16 MB pamięć flash
	7. Opóźnienia nie większe niż 1000 Mb: < 3,2 us; 10 Gb/s: < 2,6 us
	8. Przepustowość nie mniejsza, niż107,2 mln p/s
	9. Przepustowość rutowania/przełączania – co najmniej 144 Gb/s
	10. Możliwość łączenia kaskadowego IRF, 4 przełączniki
	11. IMC - Inteligent Managment Center Interfejs wiersza polecenia
	12. Przeglądarka internetowa SNMP Manager
	13. Montaż w szafie RACK (19" uchwyty w zestawie)
4. **Media konwerter – 1 szt.**
	1. Conajmniej 1 port Ethernet 1000 Mb/s na RJ-45
	2. Minimalna odległość transmisji - 15 km
	3. Funkcja auto MDI/MDI-X na porcie TX
	4. transmisja przez dwa światłowody jednomodowe
	5. Sygnalizacja optyczna wskazująca poprawność działania urządzenia
	6. W komplecie zasilacz
	7. Standardy IEE 802.3ab, IEEE 802.3z, IEE 802.3x
	8. Podstawowe funkcje Full Duplex Flow Control
	9. Interfejsy 1x1000BASE-T UTP 5, 5e (max. 100m)
	10. EIA/TIA-568 100Ω (max. 100m)
	11. 1x1000BASE-FX Jednomodowy
	12. Certyfikaty FCC, CE
	13. Okno transmisyjne [nm] 1310
	14. Zasilanie 230 V AC
	15. Minimalny zakres temperatury pracy 0-40o
5. **Skrętka UTP 305m karton – 4 szt.**
	1. skrętka - 8 żyłowy drut CCA / Al-Cu w pełni zgodny z kategorią 5
	2. możliwość tworzenia patchcordów 1Gbit/s o długości do 10m
	3. możliwość zastosowania do instalacji podtynkowych i powierzchniowych pionowych
	i poziomych, na zewnątrz i wewnątrz lokalu
	4. elastyczna osłona z samogasnącego PCV
	5. certyfikat zgodności elektromagnetycznej CE
6. **Szafa RACK stojąca 19'', 42U – 1 szt.**
	1. Minimalna wysokość robocza: 42U
	2. Rodzaj szafy: Stojąca, Jednosekcyjna
	3. wymiary [mm] (S x G x W): max:600 x max:600 x min:2055
	4. maksymalne obciążenie: co najmniej 800kg
	5. Klasa szczelności: IP20,
	6. drzwi przednie: ze szkła hartowanego lub metalowe
	7. drzwi tylnie: stalowe
	8. drzwi boczne: zamykane na zatrzask, oraz zamykane na kluczyk
	9. przepusty kablowe na przewody: od góry i od dołu
	10. Panel podłogowy: 4 kółka z hamulcem + regulowane nóżki,
	11. Panel wentylacyjny: 2 wentylatory 230V w górnej obudowie,
	12. drzwi z możliwością obrotu o 180°
	13. Zgodność ze standardami: ANSI/EIA RS-310D, IEC297-2, DIN41494; PART1 & PART7, ETSI,
	14. Grubość blachy: Profil montażowy – co najmniej: 2,00mm, Reszta – 1,2mm – 1,5mm,
	15. W zestawie: Akcesoria do mocowania, zamek drzwi przednich i tylnych, dwa zamki paneli bocznych, 20 śrub M6.
	16. Standard RACK - 19-calowy
	17. Wysokość robocza [U] – co najmniej 42U (Unit)
7. **Linka LgY 1x16 żółto-zielona – 40 m**
	1. Przewód elektroenergetyczny z izolacją PVC
	2. Linka LGY 1x16 750V H07V-K
	3. Kolor żółto-zielony
	4. Zgodność z normami PN-HD 21.3; PN-EN 50525-2-31
	5. Napięcie znamionowe: 450/750 V
	6. Napięcie próby: 2,5 kV
	7. Najwyższa dopuszczalna temp. żyły przewodzącej: co najmniej +70 °C
	8. Najwyższa dopuszczalna temp. żyły przewodzącej w warunkach zwarcia: nie mniej niż +160 °C
	9. Temperatura pracy – minimalny zakres: od -35 do +70 °C
	10. Najniższa dopuszczalna temp. układania kabli: H07V-K: +5 °C
	11. Najniższa dopuszczalna temp. przechowywania kabli: -35 °C
	12. Odporność na rozprzestrzenianie płomienia - konfiguracja pojedynczy przewód:
	IEC 60332-1-2
	13. Min. promień gięcia: 5d (średnica kabla)
	14. Certyfikat: H05V-K: EZU
	15. Zgodność z dyrektywą: RoHS
	16. Zgodność z dyrektywą: REACH
	17. Linka ma być zakończona miedzianymi, dedykowanymi końcówkami oczkowymi
8. **Patch panel 19" 5e 24p UTP patchpanel z półką - 7 szt.**
	1. Patch panel wykonany w standardzie 19” o wysokości 1U
	2. Zintegrowana półka kablowa umożliwiająca przymocowanie kabli za pomocą opasek
	i ułatwiająca rozszywanie i organizowanie kabli
	3. Co najmniej24 nieekranowane porty RJ45
	4. Złącze szczelinowe typu IDC LSA dla kabli o AWG 22 - AWG 26.
	5. Kolorowe kodowanie złącza zgodnie ze schematem rozszycia T568A i T568B.
	6. Wyposażony w elementy mocujące do szafy teleinformatycznej (komplet: śruby + podkładki + koszyczki) oraz opaski kablowe
9. **ORGANIZATOR KABLI – 12 szt.**
	1. Typ: Rack 19"
	2. Wysokość: 1U
	3. Minimalna liczba uchwytów: 12
	4. Zdejmowana metalowa płyta czołowa
	5. Komplet śrubek i koszyczków
10. **Patch cord kat.5e osłonka zalewana; 0,25m – 150 szt.**
	1. Zastosowanie: Sieciowy (LAN)
	2. Długość przewodu(Metr): 0.25 m
	3. Złącza #1: RJ45 Męska
	4. Złącza #2: RJ45 Męska
	5. Kategoria: CAT 5e
	6. Skrętka: U/UTP
	7. Kolor: 3 kolory w grupach po 50 szt.
11. **Patch cord kat.5e osłonka zalewana; 0,5m – 20 szt.**
	1. Zastosowanie: Sieciowy (LAN)
	2. Długość przewodu(Metr): 0.5 m
	3. Złącza #1: RJ45 Męska
	4. Złącza #2: RJ45 Męska
	5. Kategoria: CAT 5e
	6. Skrętka: U/UTP
	7. Kolor: różny od kolorów w punkcie 10)
12. **Patch cord kat.5e osłonka zalewana; 1m – 20 szt.**
	1. Zastosowanie: Sieciowy (LAN)
	2. Długość przewodu(Metr): 1 m
	3. Złącza #1: RJ45 Męska
	4. Złącza #2: RJ45 Męska
	5. Kategoria: CAT 5e
	6. Skrętka: U/UTP
	7. Kolor: różny od kolorów w punkcie 10) i 11)
13. **Dysk Twardy HDD 6TB – 4 szt.**
	1. Typ - dysk wewnętrzny
	2. Gwarancja36 miesięcy
	3. Pojemność (GB) 6144
	4. Format dysku 3,5"
	5. Interfejs SATA III (6 Gb/s)
	6. Pamięć podręczna64 MB
	7. Prędkość obrotowa (obr./min) 5400
	8. Dedykowany do pracy w systemach monitoringu i serwerach NAS
14. **Zasilacz UPS RACK – 1 szt.**
	1. pełna sinusoida
	2. dwustronna komunikacja i zarządzanie przez porty USB i RS232
	3. karta zdalnego zarządzania SNMP (przez WWW)
	4. możliwość rozszerzenia o zewnętrzne moduły bateryjne EBM
	5. stabilizacja napięcia AVR
	6. możliwość zasilania z generatorów prądu
	7. klasa line-interactive
	8. współczynnik mocy 0,9
	9. wyposażenie minimalne: kabel zasilający, kabel USB, oprogramowanie zarządzające
	10. Deklaracja zgodności CE GTM 1-3kVA RT
	11. Minimalna moc 1000VA / 900W
	12. WEJŚCIE –
		1. Zakres napięcia 0V – 300V
		2. Zakres częstotliwości 50Hz / 60Hz – ±5Hz
		3. Złącze wejściowe IEC C14
		4. Konektor do modułu bateryjnego
	13. WYJŚCIE –
		1. Napięcie 220V, 230V, 240V
		2. Regulacja napięcia ±5%
		3. Częstotliwość (tryb liniowy) 50Hz / 60Hz – ±5Hz
		4. Częstotliwość (tryb bat.) 50Hz / 60Hz – ±0,1Hz
		5. Współczynnik mocy (PF) 0,9
		6. Współczynnik szczytu ≥ 3:1
		7. Kształt napięcia Sinusoida
		8. Złącza wyjściowe IEC C13 (8szt.)
	14. SPRAWNOŚĆ – Tryb liniowy >96%
	15. BATERIE – Czas podtrzymania 9 min.
	16. Czas przełączenia 2-6 ms (typowy)
	17. Porty komunikacyjne EPO, RS-232, LAN (RJ45)
	18. Obudowa Rack 19” nie wyższa niż 2U
15. **Szybkozłączka podwójna do skrętki komputerowej (opakowanie 100 szt.) - 10 szt.**
	1. Żelowana
	2. UY2-4CI\*P100 umożliwia połączenie 2 przewodów
	3. Materiał: Plastik
	4. Przewód: Ø max. 1.52 mm - Powłoka zewnętrzna
	5. Żyła wewnętrzna: Ø 0.4 ... 0.7 mm
16. **Dysk sieciowy NAS -2 szt.**
	1. Procesor co najmniej 1.2GHz
	2. Pamięć nie mniejsza niż: 512MB DDR3
	3. Pamięć Flash – co najmniej 512MB
	4. Obsługa dysków: 4 x 3.5" lub 2.5" SATA 6Gb/s, SATA 3Gb/s HDD lub SSD
	5. Kieszenie na dyski: minimum 4 x Hot Swap
	6. Interfejs sieciowy: 2 RJ45 Gigabit Ethernet
	7. Porty: 3 USB 3.0 (front: 1, tył: 2), 1 eSATA (tył: 1)
	8. Obudowa: Desktop
	9. Temperatura: 0-40˚C
	10. Wilgotność: 5~95% R.H.
	11. Zasilanie: wejście: 100-240V AC, Zasilacz zewnętrzny 90W
	12. Wentylator: 1 x 120mm, 12V DC
	13. Możliwości dysku sieciowego:
		1. Dysk sieciowy / serwer plików dla Windows, MacOS, Linux (Samba)
		2. Obsługa protokołu iSCSI pozwala na obsługę bezpośrednią systemów z inicjatorem iSCSI
		3. System zastępujący klasyczny serwer Windows / Linux w firmach
		4. Kompletne rozwiązanie backupu plików z komputerów w sieci LAN
		5. Instalacja 4 dysków 3,5" lub 2,5" SATA 3, obsługa dysków do 6TB każdy
		6. Kopiowanie przez USB jednym przyciskiem z pamięci zewnętrznych i na dyski zewnętrzne
		7. Backup danych na zewnętrzne dyski i macierze poprzez interfejs USB
		8. Wbudowana funkcja zdalnej replikacji do prowadzenia szybkiego backupu
		9. Wbudowany serwer wydruku, serwer FTP oraz serwer www (php, sql, html)
		10. Pobieranie plików bez włączania PC (zarówno z Torent, FTP jak i HTTP)
		11. Zgodność z VMware, Citrix i Hyper-V
	14. Cechy pozostałe:
		1. Współpraca z Microsoft Active Directory w zakresie autoryzacji dostępu userów
		2. Szyfrowany dostęp SSL/TLS dla serwera FTP
		3. Kontrola dostępu na podstawie adresów IP (dozwolone / zabronione)
		4. Dostęp i administracja poprzez HTTPS (SSL)
		5. Szyfrowane połączenie z innymi serwerami QNAP w celu zdalnej replikacji danych
		6. Współpraca z zasilaczami awaryjnymi UPS APC
		7. Szyfrowanie całych wolumenów dyskowych kluczem AES 256bit
		8. Obsługa ACL oraz CHAP (dla iSCSI), dodatkowo LDAP i Active Directory
		9. Wbudowany serwer VPN, obsługa SSH i Telnet

**CZĘŚĆ B**

1. **Licencja PSB – 5 szt**.

Dodatkowe licencje dla jednostek centralnych na oprogramowanie Protection Service for Business
na okres 1 roku.

Istotne cechy oprogramowania:

1. Ochrona antywirusowa stacji roboczych:

- Microsoft Windows XP with SP3 (32-bit)

- Microsoft Windows Vista (32-bit i 64-bit)

- Microsoft Windows Vista with SP1 or newer (32-bit i 64-bit)

- Microsoft Windows 7 (32-bit i 64-bit)

- Microsoft Windows 7 with SP1 or newer (32-bit i 64-bit)

- Microsoft Windows 8 oraz 8.1 (32-bit i 64-bit)

- Mac OS X version 10.6 (Snow Leopard, version 10.6.8 or later)

- Mac OS X version 10.7 (Lion)

- Mac OS X version 10.8 (Mountain Lion)

1. Ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp odbywa się poprzez przeglądarkę internetową.
2. Polski interfejs użytkownika

Wymagania dotyczące technologii:

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy.
2. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.
3. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”.
4. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie plików i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.
5. Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
6. Możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
7. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.
8. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
9. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
10. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
11. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.
12. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”, „rootkit”.
13. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger”, „dialer”, „trojan” w kwarantannie.
14. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.
15. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.
16. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.
17. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.
18. Automatyczne uruchamianie procedur naprawczych.
19. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
20. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).
21. Automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem stacja robocza jest odpowiednio zabezpieczona.
22. Filtrowanie poczty e-mail – wykrywanie wiadomości typu spam oraz phisingu.
23. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.
24. Wsparcie dla technologii Microsoft Network Access Protection (NAP).
25. Ochrona przeglądarki internetowej, w tym: analiza uruchamianych skryptów ActiveX i pobieranych plików.
26. Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez producenta.
27. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.
28. Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.
29. Brak konieczności restartu systemu operacyjnego po zainstalowaniu aplikacji w środowisku Windows Vista/7/8/8.1.
30. Dostępne narzędzie do zdalnej instalacji produkty w sieci lokalnej.
31. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana.
32. Możliwość blokowania ustawień konfiguracyjnych stacji roboczych z poziomu portalu zarządzającego w celu uniemożliwienia ich modyfikacji przez użytkowników.
33. Portal zarządzający musi pozwalać na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (telefony komórkowe, smartphony).
34. Portal zarządzający dostępny w języku polskim.
35. Możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
36. Możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
37. Możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.
38. Oprogramowanie musi posiadać funkcjonalność aktualizatora aplikacji dla aplikacji firm trzecich takich jak Java, przeglądarki internetowe, klienci poczty i inne.
39. Aktualizator aplikacji musi spełniać role programu łatającego podatności a nie tylko i wyłącznie pasywnego skanera luk w bezpieczeństwie aplikacji.
40. System raportowania musi pokazywać status podatności aplikacji na komputerach dotyczące całej domeny lub pojedynczych komputerów.
41. Aktualizator aplikacji nie może wymagać instalowania dodatkowych agentów oprócz agenta AV.
42. Aktualizator aplikacji nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.

Wymagania dotyczące systemu ochrony antywirusowej dla platform mobilnych:

1. Konsola centralnego zarządzania znajdująca się na serwerach producenta oprogramowania, dostępna przez przeglądarkę internetową umożliwiająca kontrolę nad zainstalowanymi tabletami/smartfonami
2. Połączenie z konsolą za pomocą szyfrowanego połączenia AES 256-bit
3. Konsola dostępna w języku polskim
4. Możliwość importu z pliku CSV listy urządzeń, na których aplikacja ma być zainstalowana
5. Automatyczna instalacja aplikacji na urządzeniach bez konieczności wpisywania klucza na każdym instalowanym urządzeniu
6. Konsola daje administratorowi możliwość zdalnego zablokowania urządzenia oraz wykasowania danych
7. Administrator z poziomu konsoli ma możliwość odblokowania urządzenia oraz zresetowania ustawień zdalnej ochrony

Wspierane systemy operacyjne:

Android 4.0 – 5.0

Wymagania dotyczące aplikacji ochronnej dla platform mobilnych:

1. Ochrona antywirusowa realizowana na poziomie monitora kontrolującego pliki systemu operacyjnego.
2. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie.
3. Możliwość wywołania skanowania na żądanie lub według harmonogramu lokalnie określonego przez użytkownika.
4. Możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także możliwość skanowania codziennie o określonej godzinie.
5. Możliwość wywołania skanowania bezpośrednio po uruchomieniu systemu operacyjnego.
6. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (aplikacja pobiera tylko definicje, które przybyły od momentu ostatniej aktualizacji).
7. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
8. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
9. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).
10. Brak konieczności restartu urządzenia mobilnego po zainstalowaniu aplikacji w środowisku Android
11. Moduł zabezpieczający urządzenie mobilne oraz przetrzymywane na nim dane przed niewłaściwym ich użyciem w przypadku kradzieży urządzenia mobilnego.
12. Możliwość konfiguracji kodu zabezpieczającego umożliwiającego między innymi przejście użytkownika do konfiguracji oraz możliwość identyfikacji użytkownika w przypadku konieczności wykonania zdalnych akcji.
13. Możliwość konfiguracji adresu e-mail umożliwiającego odzyskanie dostępu do konfiguracji aplikacji w przypadku utraty kodu zabezpieczeń.
14. Możliwość konfiguracji zaufanego numeru telefonu, który zostanie poinformowany np. o zmianie karty SIM w chronionym urządzeniu mobilnym.
15. Możliwość zmiany kodu zabezpieczeń z poziomu konfiguracji aplikacji.
16. Możliwość zmiany blokady ekranu urządzenia mobilnego bezpośrednio z poziomu konfiguracji aplikacji.
17. Możliwość wysyłania kodów SMS z odpowiednimi komendami oraz kodem zabezpieczającym identyfikującym użytkownika.
18. Możliwość zdalnej lokalizacji urządzenia mobilnego za pomocą kodu SMS oraz kodu zabezpieczającego.
19. Możliwość zdalnego wyczyszczenia urządzenia mobilnego za pomocą kodu SMS oraz kodu zabezpieczającego.
20. Możliwość zdalnego zablokowania urządzenia mobilnego za pomocą kodu SMS oraz kodu zabezpieczającego.
21. Możliwość zdalnego uruchomienia alarmu na urządzeniu mobilnym za pomocą kodu SMS oraz kodu zabezpieczającego.
22. Możliwość konfiguracji modułu klasyfikującego wszystkie zainstalowane aplikacje, które mogą stanowić zagrożenie dla prywatności użytkownika za pomocą kryteriów takich jak dostęp aplikacji do wiadomości, dostęp aplikacji do określania lokalizacji, dostęp aplikacji do urządzeń audio/video tj. mikrofon, kamera.
23. Możliwość podglądu szczegółów wymaganych uprawnień przez daną aplikację zainstalowaną na urządzeniu mobilnym.
24. Możliwość usunięcia aplikacji uznanej przez użytkownika za niezaufaną bezpośrednio z poziomu konfiguracji modułu klasyfikującego prywatność aplikacji.
25. Możliwość konfiguracji modułu blokującego niechciane połączenia
26. Użytkownik z poziomu konfiguracji modułu blokującego niechciane połączenia może do listy blokowanych dodać ręcznie nowy numer, wybrać numer z książki telefonicznej urządzenia mobilnego lub wybrać numer z dziennika połączeń.
27. Możliwość wyświetlenia listy skonfigurowanych numerów zablokowanych dla połączeń wychodzących i przychodzących.
28. Użytkownik może wyświetlić historię blokowanych połączeń.
29. Możliwość ochrony użytkownika przed witrynami WWW mogącymi stanowić zagrożenie w postaci wykradania danych osobowych użytkownika lub zawierającymi złośliwe oprogramowanie.
30. W przypadku przejścia użytkownika na witrynę stanowiącą zagrożenie wyświetlone zostanie powiadomienie z informacją o niebezpieczeństwie.
31. Możliwość korzystania z bezpiecznej przeglądarki chroniącej prywatność użytkownika.
32. Wspierane przeglądarki przez moduł ochrony użytkownika przed niebezpiecznymi witrynami WWW:

- wbudowana przeglądarka systemu Android

- Chrome

- Dolphin

**CZĘŚĆ C**

1) **System do audytu oprogramowania oraz sprzętu, zarzadzania majątkiem, zarządzania użytkownikami, wsparcia działów IT z wbudowanym helpdeskiem z usługą serwisową na 1 rok – licencja na 100 stanowisk**

System powinien posiadać niżej wymienione cechy ogólne:

1. Oprogramowanie posiada bezterminową licencję w ramach danej wersji

2. Oprogramowanie posiada interfejs użytkownika w języku polskim.

3. Wsparcie techniczne mailowe oraz telefoniczne w języku polskim.

4. Wzajemna integracja wszystkich modułów systemu. Korzystanie z tych samych słowników, katalogu użytkowników, informacji o majątku itp.

5. System zapewnia możliwość logowania do systemu z różnymi poziomami uprawnień. System umożliwia podział bazy danych na homogeniczne całości (możliwość odizolowania np. poszczególnych jednostek organizacyjnych pod względem zarządzania w systemie oraz pracy z wynikami na podstawie uprawnień użytkowników systemu).

6. Automatyczne przypisywanie użytkowników do komputerów.

7. Podział komputerów do grup według struktury organizacyjnej, lokalizacji i użytkownika.

8. Możliwość integracji systemu z Active Directory.

9. Możliwość cyklicznej synchronizacji użytkowników, lokalizacji, jednostek organizacyjnych z Active Directory. Po synchronizacji możliwość automatycznego uruchomienia dowolnych poleceń SQL.

10. Możliwość instalacji agentów z Konsoli zarządzającej oraz możliwość dystrybucji agentów (audyt/monitoring) za pomocą GPO (paczki msi).

11. Możliwość audytu za pośrednictwem serwera FTP.

12. Możliwość pracy systemu w: sieciach rozproszonych, sieciach spiętych VPN-em, w internecie (za NAT-em). Możliwość wyboru protokołu TCP/IP lub FTP.

13. Możliwość eksportu dowolnych tabeli oraz raportów do formatów: .csv, .xls, .xlsx, .html, .pdf, .rtf, .jpeg, .png.

14. Portal webowy dla całego systemu – możliwość przeglądania wyników z audytu oraz monitoringu za pośrednictwem przeglądarki www według definiowanych uprawnień.

15. Tworzenie kopii zapasowej bazy danych bezpośrednio z konsoli programu

System powinien mieć następujące cechy audytowania

1. Możliwość przeprowadzenia audytu na komputerach z systemami Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10 ,Windows 2000 Server, Windows 2003 Server, Windows 2008 Server, Windows 2008 R2 Server, Windows 2012 Server.

2. Agent nie wymaga zewnętrznych zależności np. Microsoft .NET Framework

3. Możliwość audytowania komputerów nie podłączonych do sieci za pośrednictwem zewnętrznego nośnika (pendrive).

4. Zbieranie szczegółowych informacji o sprzęcie i jego podzespołach (procesorach, pamięciach, płytach głównych, dyskach twardych, nośnikach danych, urządzeniach WE/WY, itp.) wraz z numerami seryjnymi (lub możliwość ręcznego dopisania numerów seryjnych).

5. Identyfikacja systemu operacyjnego wraz z kluczem licencyjnym i numerem seryjnym.

6. Identyfikacja oprogramowania, a w przypadku składników pakietu MS Office identyfikacja wersji, klucza licencyjnego i numeru seryjnego (jeżeli znajduje się lokalnie na komputerze).

7. Możliwość regulacji szczegółowości rozpoznawania wersji dla każdego programu (np. możliwość grupowania 4.x lub 4.1.x, itd.)

8. Możliwość zbierania informacji o wszystkich plikach na dysku oraz możliwość definiowania dowolnych rozszerzeń

9. Możliwość uzyskiwania dodatkowych informacji z rejestrów i MSI

10. Możliwość załączenia elektronicznych dokumentów do wybranych pozycji w majątku lub licencji (faktury, dokumenty, oprogramowanie)

11. Dodatkowo system powinien mieć następujące możliwości raportowania w tym zakresie.

a. Informowanie o wygasających licencjach i gwarancjach

b. Zbiorcze statystyki audytu dla poszczególnych jednostek organizacyjnych oraz lokalizacji.

c. Raport zainstalowanego oprogramowania w sieci, zestawienia licencjonowanych i nielicencjonowanych programów

d. Rozmiar wolnego miejsca na partycjach dysków (w MB i w %)

e. Ilość, rozmiar, rozszerzenie oraz dokładna lokalizacja (ścieżka dostępu) plików danych i plików multimedialnych

f. Automatyczne porównywanie zmian pomiędzy stanem aktualnym a poszczególnymi audytami dla oprogramowania i sprzętu

g. Możliwość filtrów automatycznych, szybkiego wyszukiwania w tabelach oraz obliczeń statystycznych w kolumnach.

h. Możliwość tworzenia dokumentów dotyczących przekazania majątku, np.: protokół przekazania komputera, karta majątku itp.

i. Otwarta baza SQL (możliwość tworzenia własnych raportów – zapytań SQL bezpośrednio z programu)

j. Wbudowany możliwość tworzenia własnych raportów, możliwość pracy z szablonami raportów

System powinien mieć następujące możliwości zarządzania licencjami oraz bazą wzorców oprogramowania

1. Zarządzanie posiadanymi licencjami – bieżące śledzenie licencji i porównywanie zakupionych licencji z użytkowanymi

2. Możliwość wprowadzania licencji Upgrade, czasowych, ewidencja licencji CAL, MOLP, OEM

3. Możliwość przypisania różnych programów lub wielu wersji programu do jednej licencji.

4. Identyfikacja zainstalowanego oprogramowania na podstawie własnej bazy wzorców aplikacji, programów i pakietów

5. Bezterminowe uprawnienia do aktualizacji bazy wzorców aplikacji, programów i pakietów (bez konieczności wykupienia wsparcia, subskrypcji, abonamentu itp.).

6. Rozpoznawanie oprogramowania na podstawie wzoru generycznego (automatyczne wykrycie i rozpoznanie nowej wersji oprogramowania już wcześniej zidentyfikowanego programu)

7. Możliwość edycji bazy wzorców – tworzenie reguł, wyjątków

System powinien mieć następujące możliwości zarządzania majątkiem

1. Możliwość ewidencjonowania dowolnego sprzętu komputerowego (skaner, drukarka, pendrive, switch, telefon komórkowy itd.).

2. Możliwość zachowania danych dotyczących wycofanego komputera w bazie danych nie zajmując licencji systemu audytującego.

3. Możliwość importu sprzętu do programu z pliku csv.

4. Możliwość dodania własnych pól dla obiektu majątku.

5. Rejestrowanie napraw sprzętu.

System powinien mieć następujące możliwości zarządzania zdalnego

1. Możliwość zdalnego zarządzania stacjami: przejęcie kontroli (przejęcie obecnej sesji użytkownika), przesyłanie wiadomości, sprawdzenie jakości połączenia, możliwość kopiowania plików, przejmowanie monitora, myszy, klawiatury; zdalne wyłączanie komputera, zdalny restart.

2. Skan otwartych i zamkniętych portów.

3. Skan stanu usług w momencie audytu.

4. Zdalne zarządzanie usługami (status, sposób uruchomienia)

5. Remote Desktop Protocol – zdalny pulpit dostępny bezpośrednio z programu.

System powinien mieć następujące możliwości zdalnej instalacji oprogramowania

1. Instalacja (bez ograniczenia wielkości pliku instalacyjnego), instalacja, odinstalowanie, odinstalowanie - msi, kopiowanie, kasowanie plików i katalogów, uruchamianie skryptów lub plików, wyłączenie i restart komputera, wylogowanie użytkownika (również poza siecią lokalną).

2. Zdefiniowanie kilku serwerów, z których będą przebiegały instalacje.

3. Zdefiniowanie serii działań, które są zależne od siebie, bez poprawnego wykonania działania, następne działanie nie zostanie uruchomione.

4. Możliwość zaplanowania instalacji niezależnie od tego czy wybrane komputery są włączone lub wyłączone.

5. Przewodnik dystrybucji, który umożliwia zaplanowanie instalacji na wybranych komputerach. Zdefiniowanie dni, w których ma przebiegać instalacja oraz czasu, w którym mają być działania wykonywane.

System powinien mieć następujące możliwości zarządzania i rejestrację aktywności użytkowników

1. Rejestracja czasu pracy w aplikacji oraz czas aktywności (rzeczywisty czas aktywności użytkowników, okno (on top) na ekranie).

2. Informacje o odwiedzanych przez użytkowników stronach www: czas, statystyki wg domeny, czasu, użytkownika, konkretnych stron, czas pracy, czas aktywności użytkownika, dokładny adres strony www – aktywny odnośnik, tytuł strony.

3. Rejestracja obciążenia procesora i wykorzystania pamięci.

4. Rejestracja wydruków (jakie dokumenty, ile, z jakiej drukarki, kiedy, jaki użytkownik drukował, wysokość i szerokość kartki, liczba kopii, kolor, wydruk obustronny)

5. Rejestrowanie zmian na dyskach USB. (zmiana nazwy plików/katalogów, wielkości plików, kasowanie plików itp.)

6. Podstawowe informacje o komputerze użytkownika (dane użytkownika, nazwa komputera, zalogowany użytkownik, adres IP, adres MAC)

7. Możliwość wysyłania wyników rejestracji z dowolnego miejsca w Internecie do serwera głównego

8. Możliwość wyłączenia poszczególnych dziedzin rejestracji: www, aplikacje, obciążenie procesora, obciążenie pamięci RAM, monitoring wydruków, czas zalogowania / wylogowania użytkownika.

9. Tworzenie dowolnej ilości profili i przypisywanie ich do poszczególnych grup komputerów

10. Możliwość blokowanie aplikacji – możliwość zdefiniowania aplikacji zabronionych i uniemożliwienie ich uruchomienia, z możliwością notyfikacji mailowej na wskazany adres lub wyświetlenia okna z ostrzeżeniem na ekranie użytkownika.

11. Możliwość blokowania stron www. Dodatkowo możliwość blokowania wszystkich protokołów dla danej domeny, takich jak: http, https, ftp, imap, pop3, smtp, itp.

12. Możliwość blokowania dysków USB wg numeru seryjnego oraz sygnatury dysku.

13. Autoryzacja dysków USB - definiowanie „białej listy” dysków USB i blokowanie nieautoryzowanych.

14. Możliwość blokowania napędów CD/DVD

15. Dodatkowo system powinien mieć następujące możliwości raportowania w tym zakresie:

a. Zestawienia raportów do druku (czasowe, wg użytkownika, wg kategorii, zbiorcze, www itp.)

b. Powiadamianie (alerty) mailowo administratora np. podczas przekroczenia zdefiniowanego poziomu obciążenia RAM, procesora CPU oraz w przypadku kończącego się miejsca na dysku

c. Graficzne przedstawienie wyników za pomocą wykresów.

System powinien mieć następujące możliwości zarządzania obsługą zgłoszeń (helpdesk)

1. System umożliwia integrację z Active Directory oraz autoryzację na poziomie AD.

2. System powinien być wykonany w technologii webowej.

3. Możliwość zgłaszania problemu za pomocą maila z możliwością załączenia dowolnego załącznika

4. Integrowany moduł helpdeskowy z oprogramowaniem audytującym – wykorzystanie danych z audytu bezpośrednio w interfejsie helpdesku. Wgląd do konfiguracji (sprzęt, oprogramowanie) komputera bezpośrednio z poziomu zgłoszenia użytkownika

5. Dodatkowo system powinien mieć następujące możliwości raportowania w tym zakresie:

a. Możliwość raportowania z poziomu konsoli i przeglądarki. Raporty ilościowe, czasowe itd.

b. Ewidencja kosztów (czas, finanse) związanych ze zgłoszeniem

6. System powinien posiadać również system powiadomień zawierający poniższe cechy:

a. Wbudowany chat - możliwość dodatkowej komunikacji pomiędzy serwisantem a zgłaszającym

b. Mailowa notyfikacja użytkownika oraz serwisanta – nowe zgłoszenie, zmiana stanu zgłoszenia i inne operacje ze zgłoszeniem.

c. Automatyczna kontrola zalegających/nierozwiązanych zgłoszeń.

d. Powiadomienie meilowe (możliwość określenia treści maila w html, możliwość definicji tytułu maila, po zmianie stanu zgłoszenia, przypisaniu serwisanta, po wysłaniu wiadomości (chat)

7. Utworzenie bazy wiedzy na podstawie rozwiązanych zgłoszeń

8. Podział bazy wiedzy na część widoczną tylko dla serwisantów oraz dla wszystkich użytkowników.

9. Tworzenie własnych FAQ

10. Definiowana równych poziomów uprawnień z podziałem na użytkownik, serwisant, menadżer, administrator

11. Możliwość ustawienia trybu nieobecności serwisanta (np. urlop)

12. Możliwość załączania wielu elektronicznych załączników do zgłoszenia

13. Możliwość ustawienia dostępu do podglądu posiadanego majątku użytkownika

14. Możliwość akceptacji bądź odrzucenia przez użytkowników rozwiązania zgłoszenia

15. Możliwość oceny pracy serwisanta.

16. Możliwość wykonywania grupowych operacji na zgłoszeniach.

17. Wielopoziomowa kategoryzacja zgłoszeń – nieograniczona liczba poziomów

18. Przypisywanie serwisantów lub grup serwisantów do poszczególnych kategorii bądź podkategorii zgłoszeń

19. Możliwość określania priorytetów (czasu rozwiązania) zgłoszeń nie zależnie dla każdej kategorii lub podkategorii

20. Możliwość określenia sztywnego SLA dla każdej kategorii lub podkategorii

21. Możliwość zdefiniowania czasu pracy serwisu (przypisania różnego czasu pracy do poszczególnych kategorii i podkategorii zgłoszeń)

22. Możliwość pracy w trybie, w którym użytkownik określa termin rozwiązania wybierając datę z kalendarza

23. Możliwość określenia czasu pracy serwisu dla poszczególnych dni w tygodniu. Określony czas ma wpływ obliczanie terminu rozwiązania.

24. Możliwość przypisania dowolnych danych określonych przez administratora do wybranych kategorii zgłoszeń (można utworzyć formularz zawierający dane typu: data, łańcuch, wartość logiczna itd.)

25. Możliwość zdefiniowania ogłoszeń, które pojawią się na głównej stronie każdego użytkownika helpdesku. Możliwość integracji helpdesku z innymi systemami webowymi.

26. Formatowanie HTML w szablonach notyfikacji mailowej

27. Możliwość powiązania lokalizacji użytkownika z kategoriami - można zdefiniować kategorie, które będą widoczne tylko dla użytkowników (serwisantów) z danej lokalizacji lub jednostki organizacyjnej. Użytkownik nie wybiera lokalizacji, sam system to rozpoznaje.

28. Strukturyzowany formularz zgłoszenia różny wg kategorii (możliwość zdefiniowana pól zgłoszenia). W przypadku gdy system nie będzie tego posiadał takiej funkcji wykonawca zobowiąże się do wykonania takiej funkcji dla zamawiającego w przeciągu trzech miesięcy od dnia dostarczenia oprogramowania.

**CZĘŚĆ D**

1. **Dostawa, montaż, wdrożenie oraz przeprowadzenie szkolenia z obsługi rejestratora parametrów sieci elektrycznej w serwerowni, wraz z wymaganym osprzętem (przekładniki prądowe, itp.) – 1 szt.**

Minimalne wymagania techniczne:

| **Mierzone wielkości** |
| --- |
| **Częstotliwość**  |
| fNOM– częstotliwość nominalna | 50 / 60 Hz |
| Mierzony zakres | 42 ÷ 57 / 51 ÷ 70 Hz |
| Błąd pomiaru | +/- 20mHz |
| **Napięcie** |
| UNOM (UDIN) – (UL-N) | 180 ÷ 250 VAC |
| Mierzony zakres (UL-N) | 6 ÷ 300 VAC |
| Mierzony zakres (UL-L) | 11 ÷ 520 VAC |
| Błąd pomiaru (tA=23±2°C) | +/- 0.05 % od rdg +/- 0.02 % od rng |
| Kategoria pomiarowa | 300V CAT III |
| Przeciążalność ciągła | 1300 VAC ( UL–N ) |
| Przeciążalność w piku (UL–N / 1 sec.) | 1950 VAC ( UL–N ) |
| Pobór mocy,Rezystancja | < 0.03 VARi = 2,7 MΩ   |
| Asymetria napięciowa zakres pomiaru | 0 ÷ 10 % |
| Błąd pomiaru | +/- 0.05 % od rdg +/- 0.02 % od rng |
| THDU zakres pomiaru | 0 ÷ 20 % |
| Błąd pomiaru | +/- 0,5 |
| Harmoniczne napięcia (do 50-tej) zakres pomiaru | 10 ÷ 100 % wg IEC61000-2-4kl.3 |
| Błąd pomiaru | dwukrotny poziom z klasy II wg IEC61000-4-7 |
| **Prąd** |
| INOM (IB) – prąd wtórny znamionowy | 0.1 AAC |
| Zakres pomiaru  | 0.0025 ÷ 0.12 AAC |
| Błąd pomiaru (a=23±2°C) | +/- 0.05 % od rdg +/- 0.02 % od rng |
| Kategoria pomiarowa | 600V CAT III |
| Przeciążalność ciągła (IEC 258) | 0,2 AAC |
| Przeciążalność w piku – dla 1 sekundy, max. Częstotliwość powtórzeń > 5 minut | 1 AAC |
| Pobór mocy, (rezystancja) | < 0.005 VA ( Ri< 0,50 Ω) |
| Asymetria prądowa zakres pomiaru | 0 ÷ 100 % |
| Błąd pomiaru | +/- 1 % od rdg lub +/- 0.5 |
| THDI zakres pomiaru | 0 ÷ 200 % |
| Błąd pomiaru dla THDI < 100% | +/- 0,6 |
| Błąd pomiaru dla THDI > 100% | +/- 0,6% od rdg |
| Harmoniczne prądu (do 50-tej) zakres pomiaru | 500 % wg IEC61000-2-4 kl.3 |
| Błąd pomiaru |  Ih < 10% Inom +/- 1% InomIh > 10% Inom +/- 1% od rdg |
| **Temperatura (czujnik wewnętrzny)** |
| zakres pomiaru | -40 ÷ 80ºC |
| Błąd pomiaru  | +/- 2ºC |
| **Pomiar energii** |
| zakres pomiaru | 6-kwadrantowy, koresponduje z zakresami pomiaru napięcia i prądu |
| Błąd pomiaru dla energii czynnej | kl.1 wg EN62053-21 |
| Błąd pomiaru dla energii biernej | kl.2 wg EN62053-23 |

|  |
| --- |
| **Pozostałe dane techniczne** |
| Temperatura pracy | - 20 to 60°C |
| Temperatura składowania | - 40 to 80°C |
| Wilgotność | < 95 % - bez kondensacji |
| EMC – odporność | EN 61000 – 4 - 2 ( 4kV / 8kV ); EN 61000 – 4 - 3 ( 10 V/m up to 1 GHz );EN 61000 – 4 - 4 ( 2 kV ); EN 61000 – 4 - 5 ( 2 kV );EN 61000 – 4 - 6 ( 3 V ); EN 61000 – 4 - 11 ( 5 periods ) |
| EMC – emisja | EN 55011, class A EN 55022, class A (nie do użycia domowego) |
| Port zdalnej komunikacji (opcja) | RS-485 opcjonalnie USB, Ethernet, Zig Bi, Wi-Fi |
| Protokół komunikacyjny  | KMB, Modbus-RTU lub TCP, DHCP, webserver |
| Dokładność RTC | +/- 2 sek. na dzień |
| Trwałość baterii dla RTC | > 5 lat (bez zasilania pomocniczego) |
| Pamięć do zapisu danych  | 512 Mb z interwałem zapisu od 200ms do 24h |
| Stopień ochrony : panel przednizaciski | IP 40 ( IP 54 z osłoną )IP 20 |

|  |  |
| --- | --- |
| **Cyfrowe wyjścia & cyfrowe wejścia** |  |
| **Wyjścia - półprzewodnik, opto-MOS** |
| Typ | Opto-MOS,  |
| Obciążalność | 100 VDC, 300 mA |
| **Cyfrowe wejście** |
| Typ | optoizolowane, |
| Maksymalne napięcie | 30 VDC |
| Napięcie dla “logicznej 1“ | > 10 VDC  |
| Napięcie dla “logicznego 0“ | < 3 VDC  |
| Prąd wejściowy | 1 mA @ 10V / 8 mA @ 24V  |

Ponad to:

a) Cztery niezależne wejścia napięciowe i prądowe

b) Pośrednia i bezpośrednia możliwość pomiarów napięcia

c) Możliwość pomiaru prądów do 600A za pośrednictwem przekładników prądowych

d) Obsługa 3 taryf jednofazowych

e) Interwał pomiarowy 10/12 okresu, 128 próbek/okres

f) Rejestrator z 512 Mb pamięci flash do odczytów parametrów sieci

g) Opcje zasilania (U:75-510 VAC, 80-350 VDC, L:20-75 VDC, 24-48 VAC)

h) Programowalne wyjście cyfrowe

i) Interfejs RS-485

j) Wymagana komunikacja siecią Ethernet 10/100 Base-T

k) Opcjonalnie moduł rozszerzeń z siecią M-Bus

l) Opcjonalnie moduł rozszerzeń z USB

m) Opcjonalnie moduł rozszerzeń z WiFi

n) Klasa pomiaru 0,5

Zabezpieczenie główne w serwerowni – 3 x 100A