

Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA



Spis treści:

- I. Zakup serwera NAS wraz z instalacją i konfiguracją - GOPS (szt. 1)
- II. Zakup Agregatu prądowórczego wraz z instalacją (szt. 1)
- III. Zakup UTM z wdrożeniem - GOPS (szt. 1)
- IV. Zakup oprogramowania antywirusowego
- V. Zasilacz UPS - GOPS (szt. 1)
- VI. Zasilacz UPS - Urząd Gminy (szt. 1)

I. Zakup serwera NAS wraz z instalacją i konfiguracją - GOPS (szt. 1)

WYMAGANIA MINIMALNE:

- **Pamięć RAM 32 GB**
- **Dyski twarde – 4 szt. po 8TB każdy**
- 2 gniazda dysków M.2 NVMe
- Wbudowany podwójny szybki interfejs sieciowy - 2.5GbE z obsługą funkcji Link Aggregation przełączania awaryjnego
- Panel użytkownika i oprogramowanie dostępne w języku polskim
- Wbudowane systemy zabezpieczeń sieciowych, antywirus, szyfrowanie AES 256bit oraz dwustopniowe uwierzytelnianie użytkowników
- 2 porty USB 3.2 Gen 1
- Wbudowany serwer VPN oraz SQL
- Dostęp do danych za pomocą aplikacji mobilnych z telefonu lub tabletu
- Możliwość podłączenia jednostki rozszerzającej
- Wbudowany serwer FTP z funkcjami SSL, TLS
- Obsługa Windows AD, LDAP oraz Domain Trust
- USB-Copy i kompleksowy backup danych na serwer i urządzenia zewnętrzne
- Możliwość zbudowania systemu monitoringu z kamerami IP

PARAMETRY SZCZEGÓŁOWE (minimalne):

Procesor	Model CPU	Procesor umożliwiający osiągnięcie wyniku min. 4500 punktów teście PassMark CPU Benchmarks dostępnym na stronie https://www.cpubenchmark.net/cpu_list.php
	Liczba procesorów	1
	Rdzeń procesora	4
	Architektura procesora	64-bitowym
	Częstotliwość procesora	2.2 GHz
	Mechanizm szyfrowania sprzętowego	Tak
Pamięć	Pamięć systemowa	32 GB DDR4 ECC SODIMM
	Całkowita liczba gniazd pamięci	2
	Maksymalna pojemność pamięci	32 GB (16 GB x 2)
Pamięć	Kieszeń/kieszenie na dyski	4
	Maks. liczba kieszeni na dyski z jednostką rozszerzającą	9 (DX525 x 1)
	Kieszenie dysków M.2	2 (NVMe)
	Typ dysku	3.5" SATA HDD - Dysk SATA SSD 2,5" - M.2 2280 NVMe SSD



	Dysk z możliwością wymiany podczas pracy (hot-swap)*	Tak
	Uwagi	- Funkcja wymiany dysków podczas pracy nie jest obsługiwana przez gniazda M.2 SSD. - Kompatybilne dyski są obowiązkowe.
Porty zewnętrzne	Port LAN RJ-45 2.5GbE	2
	Port USB 3.2 1. generacji	2
	Gniazdo rozszerzenia	1
	Typ portu rozszerzeń	USB Type-C
Inne		
	Tryb prędkości wentylatora	- Tryb pełnej prędkości - Tryb chłodzenia - Tryb cichy
	Kontrolki LED z regulacją jasności	Tak
	Przywracanie zasilania	Tak
	Zaplanowane włączanie/wyłączanie	Tak
	Funkcja Wake on LAN / WAN	Tak
	Zasilacz / Adapter	100 watów
	Napięcie wejściowe zasilania prądem zmiennym	100V to 240V AC



	Częstotliwość zasilania	50/60 Hz, Jednofazowy
	British thermal unit	129.27 BTU/hr (dostęp) 42.05 BTU/hr (hibernacja dysków twardych)
Temperatura	Temperatura pracy	0°C do 40°C (32°F do 104°F)
	Temperatura przechowywania	-20°C do 60°C (-5°F do 140°F)
	Wilgotność względna	5% do 95% RH
Certyfikaty	• FCC • CE • BSMI • VCCI • RCM • UKCA • EAC • CCC	
Gwarancja	3-letnia gwarancja na sprzęt, z możliwością rozszerzenia do Przedłużonej Gwarancji Plus	
Środowisko	Zgodność z dyrektywą RoHS	

1. Specyfikacja dysków SATA do serwera NAS – 4 szt.

Sprzęt		
Ogólne	Pojemność	8 TB
	Obudowa	3.5"
	Interfejs	SATA 6 Gb/s
Wydajność	Prędkość obrotowa	7.200 rpm
	Maksymalna stała prędkość przesyłu	260 MB/s

	danych (typ.)	
Niezawodność	Gwarancja	3 lata
	Uwagi	Okres gwarancyjny rozpoczyna się od daty zakupu podanej na paragonie zakupu.
Zużycie energii	Aktywny tryb bezczynności (typ.)	5.61W
	Losowy odczyt/zapis (4 KB Q1) (typ.)	8.41W
	Uwagi	Zużycie energii może się różnić w zależności od konfiguracji i platform.
Temperatura	Działa	5°C do 65°C (41°F do 149°F)
	Nie działa	-40°C do 70°C (-40°F do 158°F)

II. Zakup Agregatu prądotwórczego wraz z instalacją (szt. 1)

PARAMETRY MINIMALNE:

1) Parametry silnika

- Klasa G2
- Silnik wysokoprężny, 4-suwowy napędzany olejem napędowym
- Chłodzony cieczą (Chłodnica)
- Moc silnika 29kW
- Ilość obrotów podczas pracy 1500, automatyczna regulacja
- Konfiguracja silnika - Rzędowy (R4) z bezpośrednim wtryskiem
- Regulacja obrotów - Tak, mechaniczna
- Pojemność skokowa 2.545cc3
- Pojemność miski olejowej 8L
- Spalanie na poziomie 230 (g/kW.h)
- Rozrząd zaworowy napędzany kołem zębatym
- Silnik z pompą olejową (wymuszone smarowanie)
- Rozrusznik elektryczny
- Podgrzewacz bloku silnika oraz cieczy chłodzącej
- Pomiar obciążenia oraz napięcia na każdej fazie
- Czujnik poziomu oleju, ciśnienia oleju, temperatury wody



- Pomiar poziomu paliwa, napięcia akumulatora, licznik motogodzin
- Ładowanie akumulatorów w czasie postoju - TAK
- Automatyczny system zabezpieczający agregat (asymetria, napięcie, przeciążenie)
- Funkcja automatycznego rozruchu (SZR)

2) Parametry prądnicy

- Moc maksymalna - 24 kW (30kVA)
- Moc znamionowa - 20 kW (25kVA)
- Prąd nominalny 36A / 1 fazę
- Uzwojenia wykonane z miedzi
- Synchroniczna bezszczotkowa, 50Hz
- Napięcie wyjściowe 400V/230V
- Zabezpieczenie C50
- Samowzbudna
- Samokontrola i stabilizacja napięcia (AVR)

3) Parametry obudowy

- Wymiary maksymalne: 185(dł) x 75(sz) x 85cm(w)
- Waga agregatu netto: max 620 kg
- Szczelna obudowa IP-44
- Stalowa wyciszona konstrukcja (max 73dB)
- Zbiornik paliwa o pojemności minimum 45 litrów
- Platforma absorbująca drgania
- Łatwy dostęp do płynów eksploatacyjnych

4) Dodatkowe wymagamy

1. Deklaracji zgodności WE
2. Podstawowego szkolenie z obsługi agregatu prądotwórczego
3. Gwarancji 36 miesięcy
4. Gotowości agregatu do pracy (zalaný olejem silnikowym oraz płynem chłodniczym)
5. Możliwości wymiany olejów oraz filtrów we własnym zakresie bez utraty gwarancji



6. Podłączenia do istniejącej instalacji elektrycznej w budynku Urzędu Gminy Radków z uwzględnieniem miejsca posadowienia agregatu w garażu Urzędu Gminy oddalonym o ok. 30m od złącza głównego sieci budynku.
7. Uwzględnienie przy pracach podłączeniowych agregatu istniejącej instalacji PV .

III. Zakup UTM z wdrożeniem - GOPS (szt. 1)

MINIMALNE PARAMETRY UTM-a

1) OBSŁUGA SIECI

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

2) ZAPORA KORPORACYJNA (Firewall)

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.

9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

3) INTRUSION PREVENTION SYSTEM (IPS)

1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
9. Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

4) KSZTAŁTOWANIE PASMA (Traffic Shapping)

1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.

2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

5) OCHRONA ANTYWIRUSOWA

1. Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie.
2. Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania).
3. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.
4. Skaner antywirusowy ma pochodzić od europejskiego producenta.
5. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
6. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

6) OCHRONA ANTYSZPAM

1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
2. Ochrona antyspam ma działać w oparciu o: białe/czarne listy, DNS RBL,
3. Skaner heurystyczny.
4. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

7) WIRTUALNE SIECI PRYWATNE (VPN)

1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: PPTP VPN, IPSec VPN, SSL VPN.
3. SSL VPN ma działać w trybie tunelu.
4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łączy zapasowe na wypadek awarii łączy dostawcy podstawowego (VPN Failover).
7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
8. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

8) FILTR DOSTĘPU DO STRON WWW

1. Urządzenie ma posiadać wbudowany filtr URL.
2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych.
3. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.
4. Administrator ma mieć możliwość dodawania własnych kategorii URL.
5. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
 6. blokowanie dostępu do adresu URL,
 7. zezwolenie na dostęp do adresu URL,
 8. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
9. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
10. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
11. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
12. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.

- 13 Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
- 14 Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.

9) UWIERZYTELNIANIE

1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: lokalną bazę użytkowników (wewnętrzny LDAP), zewnętrzną bazę użytkowników (zewnętrzny LDAP), usługę katalogową Microsoft Active Directory.
2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: SSL, Radius, Kerberos.
4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
10. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.

10) ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: równoważenie względem adresu źródłowego, równoważenie względem połączenia.

3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łączy podstawowego (tzw. Failover).
5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łączy.
6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów).
7. Monitorowanie dostępności łączy musi być możliwe w oparciu o ICMP oraz TCP.

11) ROUTING (TRASOWANIE)

1. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łączy podstawowego.
3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
5. Rozwiązanie musi dawać możliwość wybrania predefiniowanego obiektu typu blackhole.

12) ADMINISTRACJA URZĄDZENIEM

1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
6. Urządzenie ma umożliwiać zarządzanie z poziomu konsoli (SSH)
7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.

8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
17. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: manualnego eksportu do pliku w dowolnym momencie czasu, automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

13) RAPORTOWANIE

1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.

3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

14) POZOSTAŁE USŁUGI I FUNKCJE

1. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
2. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
3. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
4. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
5. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
6. Urządzenie ma posiadać usługę DNS Proxy.
7. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
8. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
9. Urządzenie musi mieć zaimplementowane Open API.
10. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
11. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.

15) GWARANCJA I SERWIS

1. Urządzenie ma być objęte 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

16) PARAMETRY SPRZĘTOWE

1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
2. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
3. Liczba portów Ethernet 2,5Gbps – min. 8.
4. Liczba portów światłowodowych 1Gbps – min. 1.
5. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
6. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
7. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.
8. Przepustowość filtrowania Antywirusowego – minimum 500Mbps.
9. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
10. Liczba tuneli VPN IPSec – minimum 100.
11. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
12. Obsługa interfejsów 802.11q (VLAN) – minimum 128
13. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.
14. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
15. Urządzenie nie ma limitu na liczbę użytkowników.
16. Liczba reguł filtrowania – minimum 8 192.
17. Liczba tras statycznego routingu – minimum 512.
18. Liczba tras dynamicznego routingu – minimum 10 000.
19. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne).
Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
20. Urządzenie musi być wyposażone w moduł TPM.

IV. Zakup oprogramowania antywirusowego

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	Zamawiający posiada licencje antywirusa GravityZone Business Security 25 użytkowników. Wymaga przedłużenia posiadanej licencji o 12 miesięcy. Zamawiający dopuszcza dostarczenia rozwiązania równoważnego, spełniającego podane poniżej wymagania. W przypadku dostarczenia rozwiązania równoważnego, zamawiający wymaga: -odinstalowania posiadanego rozwiązania -pełnego wdrożenia i skonfigurowania rozwiązania równoważnego -przeszkolenia administratora z dostarczonego rozwiązania równoważonego, w wymiarze minimum 8h.
Wymagania równoważności	Ochrona antywirusowa i antyspyware 1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim 3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi 4. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog 5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 6. Wbudowana technologia do ochrony przed rootkitami. 7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 10. Możliwość skanowania dysków sieciowych i dysków przenośnych. 11. Skanowanie plików spakowanych i skompresowanych. 12. Możliwość dodawania wykluczeń na podstawie a) Plik

- b) Folder
- c) Rozszerzenie
- d) Proces
- e) Hash pliku
- f) Hash certyfikatu
- g) Nazwa zagrożenia
- h) Wiersz poleceń
- i) IP/maska

13. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.

14. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

15. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.

16. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.

17. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.

18. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.

19. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.

20. Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH

21. Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.

22. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.

23. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji: O

programie” możliwość wyświetlenia danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.

24.W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.

25.W GUI programu możliwość wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia.

26.Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.

27.Obługa pobierania aktualizacji za pośrednictwem serwera proxy.

28.Praca programu musi być niezauważalna dla użytkownika.

29.Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.

30.Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.

31.Oprogramowanie klienckie posiada wbudowaną funkcję do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.

32.Możliwość odblokowania ustawień programu po wpisaniu hasła

33.Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu.

34.Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie).

35.Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu.

36.Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.).

37.Funkcja Ochrony danych konfigurowana zdalnie przez administratora.

38.Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.

39.Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.

40.Wbudowany IDS.

41. Możliwość zainstalowania silnika pełnego lub lekkiego ze sprawdzaniem reputacji plików w chmurze.
42. Możliwość tworzenia list sieci zaufanych.
43. Możliwość dezaktywacji funkcji zapory sieciowej.
44. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
45. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
46. Mechanizm, który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji.
47. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa).
48. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups.
49. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.
50. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać:
- a) Funkcję, która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:
- Ochrony przeglądarki internetowej
 - Sieć i poświadczenia
 - Błędna konfiguracja systemu operacyjnego
- System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.
- b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.
- c) System, który pozwala na śledzenie i wykrywanie niezwykłych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.
- d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na

podstawie harmonogramu lub pojedynczo utworzonego zadania.

e)System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.

f)System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie

51.Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:

a)Możliwość wymuszenia funkcji DEP systemu Windows

b)Możliwość wymuszenia relokacji modułów (ASLR)

Uwaga: Ta warstwa zabezpieczeń dotyczy systemów opartych na systemie Windows.

52.Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak:

-Wczesny dostęp

-Dostęp do poświadczeń

-Wykrycie

-Crimeware

53.Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.

54.Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.

Formaty plików jakie mogą być odzyskane:

3fr|ai|arw|bay|cab|cdr|cer|cr2|crt|crw|dcr|der|dgn|dll|dng|doc|docm|docx|dwg|dxf|dxg|eps|erf|exe|indd|ini|jpe|jpeg|jpg|mdf|mef|mrw|msg|msi|nef|nrw|odb|odc|odm|odp|ods|odt|orf|p12|p7b|p7c|pdd|pdf|pef|pem|pfx|png|ppt|pptm|pptx|psd|pst|ptx|py|r3d|raf|rtf|rw2|rwl|sr2|srf|srw|tsf|wb2|wpd|wps|x3f|xlk|xls|xlsb|xls|xsm|xlsx|xml|

Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego

odzyskiwania.

55.System musi wykrywać podatne sterowniki zainstalowane na punkcie końcowym

56.Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności.

57.Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows

58.System musi umożliwiać skanowanie oprogramowania układowego UEFI

Stacje robocze i serwery

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.

2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.

3. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".

5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.

6. Skanowanie plików spakowanych i skompresowanych.

7. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.

8. Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu.

9.Produkt i sygnatury są aktualizowane nie rzadziej niż raz na godzinę.

10.Oprogramowanie posiada możliwość raportowania zdarzeń informacyjnych.

11.Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.

12.Program musi posiadać możliwość skanowania jedynie nowych niezmienionych plików.

13.Program musi mieć wbudowany skaner wyszukiwania rootkitów.

14.Możliwość odblokowania ustawień programu po wpisaniu hasła.

15. Możliwość uruchomienia zadania skanowania z niskim priorytetem.
16. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu).
17. Możliwość określenia jak długo mają być przechowywane zdarzenia na stacji roboczej.
18. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem
19. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
20. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.

Konsola zdalnej administracji

1. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.
2. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.
3. Możliwość integracji wielu domen Active Directory
4. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
5. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
6. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi
7. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.
8. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internet
9. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
10. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.



11. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.

12. Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv.

13. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.

14. Możliwość generowania raportu co godzinę.

15. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.

16. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.

17. Możliwość dodania etykiety do stacji roboczej.

18. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.

19. Możliwość przechowywania kwarantanny maksymalnie 180 dni

20. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.

21. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.

22. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.

23. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym.

24. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.

25. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.

26. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie

- Zakres adresów IP/IP

- Adres bramy

- Adres serwera WINS

- Adres serwera DNS



-Połączenie DHCP sufiksów DNS

-Punkt końcowy może rozwiązać hosta

-Typ sieci

-Nazwa hosta

27.Integracja z serwerem Syslog.

28.Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238

29.Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.

30.Możliwość zablokowania konta w konsoli, jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.

31.Funkcja pojedynczego logowania – Single Sign-on (SSO).

32.Możliwość naprawy instalacji z poziomu konsoli.

33.Raport streszczający - Możliwość podglądu raportu, który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:

-Zarządzane punkty końcowe

-Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne

-Pięć najczęściej blokowanych zagrożeń

-Podział zagrożeń na urządzenia takie jak stacje robocze i serwery

-Status incydentów bezpieczeństwa, które wystąpiły

-Stan modułów punktów końcowych

-Ocena ryzyka firmy

-Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.

-Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware

34.Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:

a)Pakiety

b)Sieć

c)Kwarantanna



d)Licencjonowanie

e)Integracje

f)Polityki

g)Raporty

h)Konta

i)Firmy

35.Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej, jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn, które automatycznie będą usuwane oraz pozwala na określenie godziny, kiedy te maszyny będą usuwane

36.Możliwość określenia własnego serwera NTP.

37.Integracja z vCenter Server.

38.Integracja z Xen Server.

39.Integracja z nutanix Prism Element.

40.Możliwość integracji z Amazon EC2

41.Integracja z Azure.

42.Pion firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej, dostępne muszą być opcje takie jak:

a)Lotnictwo

b)Rolnictwo

c)Automotive

d)Usługi komercyjne

e)Doradztwo

f)Energia

g)Usługi finansowe

h)Rząd

i)Opieka zdrowotna

j)Technologie

k)Transport

l)Non-profit

m)Górnictwo

n)Media



43.Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.

44.Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.

45.Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS

46.Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.

47.Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.

48.Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS

Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1.

49.Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.

50.Program testowy – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Programy wczesnego dostępu powinny umożliwiać testowanie najnowszych funkcji oprogramowania których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.

51.Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Przypisywanie musi odbywać się ręcznie lub automatycznie. Musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.

52.System umożliwia pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli administracyjnej.

Konsola Cloud – serwer administracyjny po stronie producenta

1. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać:

a) Funkcję, która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:

- Ochrony przeglądarki internetowej
- Sieć i poświadczenia
- Błędna konfiguracja systemu operacyjnego

System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.

b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.

c) System, który pozwala na śledzenie i wykrywanie niezwykłych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.

d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.

e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.

f) System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie.

2. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.

a) Możliwość zablokowania konta w konsoli, jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.

b) Funkcja pojedynczego logowania – Single Sign-on (SSO).

c) Możliwość naprawy instalacji z poziomu konsoli.

d) Raport streszczający - Możliwość podglądu raportu, który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:

- Zarządzane punkty końcowe
- Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne
- Pięć najczęściej blokowanych zagrożeń
- Podział zagrożeń na urządzenia takie jak stacje robocze i serwery
- Status incydentów bezpieczeństwa, które wystąpiły
- Stan modułów punktów końcowych

-Ocena ryzyka firmy

-Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.

-Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware.

3. Pion firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej, dostępne muszą być opcje takie jak:

- a) Lotnictwo
- b) Rolnictwo
- c) Automotive
- d) Usługi komercyjne
- e) Doradztwo
- f) Energia
- g) Usługi finansowe
- h) Rząd
- i) Opieka zdrowotna
- j) Technologie
- k) Transport
- l) Non-profit
- m) Górnictwo
- n) Media

4. Możliwość integracji sekcji Firmy z innymi systemami poprzez API.

5. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.

6. Program testowy – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Programy wczesnego dostępu powinny umożliwiać testowanie najnowszych funkcji oprogramowania których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.

7. Możliwość utworzenia konsoli typu Partner, która pozwala na zarządzanie wieloma firmami z poziomu jednej scentralizowanej konsoli zarządzającej, konsola partnerska

	musi umożliwiać: a) Możliwość pobierania przez partnera plików z kwarantanny podległych firm
Ilość	1 sztuka

V. Zasilacz UPS - GOPS (szt. 1)

Specyfikacja (wymagania minimalne):

- | | |
|---|---|
| 1. Topologia: | Line-interactive |
| 2. Moc pozorna: | 3000 VA |
| 3. Moc skuteczna: | 3000 W |
| 4. Napięcie wejściowe: | 178 - 281 V |
| 5. Kształt napięcia wyjściowego: | Sinusoidalny |
| 6. Gniazda wyjściowe: | 230 V EU - 2 szt. |
| | IEC 320 C13 (sterowalne) - 3 szt. |
| | IEC 320 C13 - 3 szt. |
| | IEC 320 C19 - 1 szt. |
| | RJ-45 |
| | USB |
| 7. Czas przełączania: | 3 ms |
| 8. Czas podtrzymania dla obciążenia 50%: | 7 min |
| 9. Czas podtrzymania dla obciążenia 100%: | 3 min |
| 10. Średni czas ładowania: | 4 h |
| 11. Interfejs komunikacyjny: | USB |
| 12. Zabezpieczenia: | Przeciwzwarciove |
| | Przeciążeniowe |
| | Przeciwprzepięciowe |
| 13. Sygnalizacja pracy: | Wyświetlacz LCD |
| | Dźwiękowa |
| 14. Typ obudowy: | Tower/Rack |
| 15. Dodatkowe informacje: | Możliwość pracy w pozycji pionowej lub poziomej |
| | Wbudowany wyświetlacz LCD |
| 16. Gwarancja na urządzenie: | 36 miesięcy |
| 17. Gwarancja na akumulatory: | 24 miesiące |

18. Wyjściowa moc czynna równa mocy pozornej
19. System regulacji napięcia sieciowego AVR
20. Układ ładowania akumulatorów z kompensacją termiczną
21. Predykcja czasu podtrzymywania
22. Zimny start Interfejs sieciowy w standardzie Interfejs komunikacyjny HID USB
23. Dodatkowy moduł bateryjny Interfejs komunikacyjny RS232/RS485 z protokołem MODBUS

VI. Zasilacz UPS - Urząd Gminy (szt. 1)

Specyfikacja (wymagania minimalne):

- | | |
|---|--|
| 1. Topologia: | Line-interactive |
| 2. Moc pozorna: | 3000 VA |
| 3. Moc skuteczna: | 3000 W |
| 4. Napięcie wejściowe: | 178 - 281 V |
| 5. Kształt napięcia wyjściowego: | Sinusoidalny |
| 6. Gniazda wyjściowe: | 230 V EU - 2 szt.
IEC 320 C13 (sterowalne) - 3 szt.
IEC 320 C13 - 3 szt.
IEC 320 C19 - 1 szt.
RJ-45
USB |
| 7. Czas przełączania: | 3 ms |
| 8. Czas podtrzymania dla obciążenia 50%: | 7 min |
| 9. Czas podtrzymania dla obciążenia 100%: | 3 min |
| 10. Średni czas ładowania: | 4 h |
| 11. Interfejs komunikacyjny: | USB |
| 12. Zabezpieczenia: | Przeciwzwarceniowe
Przeciążeniowe
Przeciwprzepięciowe |
| 13. Sygnalizacja pracy: | Wyświetlacz LCD
Dźwiękowa |
| 14. Typ obudowy: | Tower/Rack |
| 15. Dodatkowe informacje: | Możliwość pracy w pozycji pionowej lub poziomej |

Wbudowany wyświetlacz LCD

- 16. Gwarancja na urządzenie: 36 miesięcy
- 17. Gwarancja na akumulatory: 24 miesiące
- 18. Wyściowa moc czynna równa mocy pozornej
- 19. System regulacji napięcia sieciowego AVR
- 20. Układ ładowania akumulatorów z kompensacją termiczną
- 21. Predykcja czasu podtrzymywania
- 22. Zimny start Interfejs sieciowy w standardzie Interfejs komunikacyjny HID USB
- 23. Dodatkowy moduł bateryjny Interfejs komunikacyjny RS232/RS485 z protokołem MODBUS

