Część 1. Dostawa oprogramowania do wykonywania kopii zapasowych wraz z gotową macierzą - 1 kpl.

Wymagane i oferowane funkcje oprogramowania

Lp.	Temat	Wymagane funkcje oprogramowania
1.	**Ogólne**	1. System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu, 2. Interfejs systemu dostępny jest w języku: a) polskim, b) angielskim 3. System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji w środowisku lokalnym oraz, z możliwością odtworzenia w postaci usługi uruchomionej w chmurze producenta zlokalizowanej na terenie Polski, 4. Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej), 5. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
2.	**Wsparcie techniczne**	1. Pomoc techniczna w językach: 2. Świadczone jest bezpośrednio przez główną siedzibę producenta, 3. Materiały samopomocowe a) Baza wiedzy, b) Nagrania wideo, c) Karty produktowe
3.	**Zarządzanie**	1. Zarządzanie całością działania systemu (backup, przywracanie) z poziomu jednej konsoli, dostępnej za pośrednictwem przeglądarki WWW, 2. Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego, 3. Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem, 4. Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem, 5. Monitorowanie postępu działania zadania, 6. Posiada system powiadamiania poprzez e-mail bądź Slack o zdarzeniach w następujących przypadkach: a) Zadanie zostało zakończone pomyślnie, b) Zadanie zostało zakończone z ostrzeżeniami, c) Zadanie zostało zakończone z błędem, d) Zadanie zostało anulowane, e) Zadanie nie zostało uruchomione 7. System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego, 8. System umożliwia wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika, 9. Możliwość zdefiniowania okna backupowego dla każdego z zadań, 10. Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów i innych sekretów, wykorzystywanych przez System, 11. System pozwala na klonowanie planów kopii zapasowych, 12. System umożliwia reset hasła administratora w przypadku jego utraty, 13. Oprogramowanie umożliwia definiowanie retencji według schematów: a) GFS(Grandfather-Father-Son), b) FIFO(First-In, First-Out), 14. Oprogramowanie umożliwia tworzenie grup urządzeń, 15. Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów), 16. System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: a) System Administrator, b) Backup operator, c) Restore operator, d) Viewer,
4.	**Składowanie danych**	1. Dane są składowane w ramach dostępnej macierzy wymienionej w wymaganiach sprzętowych OPZ (wymagania poniżej), 2. Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach: a) Lokalnie: - Zasób SMB, - Zasób NFS,

		- Zasób ISCSI, - Zasób S3, - Katalog zabezpieczonego urządzenia, b) W Chmurze: - Amazon Web Service, - Magazyn zgodny z S3, - Dostarczanej przez producenta, 3. System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle, 4. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami, 5. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych, 6. System obsługuje mechanizm WORM (Write Once Ready Many) w chmurowych oraz lokalnych repozytoriów kopii,
5.	**Odtwarzanie**	1. Kopie zapasowe powinny móc być odtwarzane przy wykorzystaniu zasobów sprzętowych dostarczanej macierzy przy wykorzystaniu narzędzi Disaster Recovery dołączonych do oprogramowania, 2. Odtwarzanie granularne: a) Pojedynczych plików z kopii obrazu dysku, b) Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365, 3. Wykorzystanie funkcjonalności Bare Metal Restore (kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów: a) Windows: 7+, b) Windows Server: 2008 R2+, 4. Odtwarzanie Bare Metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika, 5. Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a, 6. Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V, 7. Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK), 8. Odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL), 9. Odtwarzanie zasobów plikowych z prawami dostępu, 10. Przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows), 11. Odtwarzanie danych według harmonogramu, 12. Przywracanie danych z określonego urządzenia/użytkownika, 13. Przywracanie kopii z wybranego magazynu. 14. Przywracanie danych Microsoft 365: a) do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst b) do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji), 15. System posiada możliwość nieodwracalnego kasowania danych, 16. Przywracanie repozytoriów GIT: a) przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket/GitLab), b) przywracanie między kontami,
6.	**Backup**	1. Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych dla: a) Systemów operacyjnych: - Alpine 3.10+, - Debian: 9+, - Ubuntu: 16.04+, - Fedora: 29+, - centOS: 7+, - RHEL: 6+, - openSUSE: 15+, - SUSE Enterprise Linux(SLES): 12 SP2+, - macOS: 10.13+, - Windows: 7 i nowsze, - Windows Server: 2008 R2 i nowsze, b) Środowisk wirtualnych: - Hyper-V, - VMware, - Dowolnych innych – agentowo, c) Repozytoriów GIT: - GitHub, - Bitbucket, - GitLab d) Jira Cloud: 2. Wykonywanie pełnych, różnicowych oraz przyrostowych kopii zapasowych dla: a) Baz danych: - Microsoft SQL, - MySQL, - PostgreSQL, - Firebird, - Oracle, - Dowolnych innych przez podpięcie skryptów pre/post.

		3. Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości: a) 128 bit, b) 192 bit, c) 256 bit, 4. Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów: a) ZStandard, b) LZ4, 5. Oprogramowanie umożliwia zarządzanie poziomem kompresji, 6. System dostarcza agenta backupu w postaci kontenera Docker, umożliwiającego wykonywanie kopii zapasowych z dowolnych środowisk kontenerowych, w tym popularnych rozwiązań NAS, 7. System dostarcza agenta backupu w postaci instalatora MSI, umożliwiającego masową instalację w systemach Windows z wykorzystaniem narzędzi Active Directory - SCCM oraz GPO 8. Wykonywanie kopii zapasowej otwartych plików (VSS), 9. System umożliwia uruchamianie skryptów przed i po backupie, 10. System umożliwia uruchamianie skryptów po wykonaniu migawki VSS, 11. System umożliwia wykonywanie spójnej kopii danych pracujących aplikacji na urządzeniach z systemem Windows oraz wspieranych środowiskach wirtualnych, 12. System pobiera jedynie zmodyfikowane bloki danych podczas przyrostowej i różnicowej kopii maszyn wirtualnych VMware, 13. System umożliwia wykonywanie kopii maszyn wirtualnych VMware z zastosowanie zaawansowanych trybów transportu (HotAdd, LAN, SAN), w tym metodą LAN-Free, 14. System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów, 15. Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT, 16. Backup plikowy, 17. Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe, 18. Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia, 19. Oprogramowanie pozwala na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej, 20. Oprogramowanie pozwala na backup zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption,
7.	**GIT**	1. Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych (dostępnych w usługach zewnętrznych), 2. Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki),
8.	**Licencjonowanie**	1. Licencje powinny pozwalać na zabezpieczenie: a) Nielimitowanej ilości maszyn wirtualnych, b) Nielimitowanej ilości serwerów fizycznych, c) Nielimitowanej ilości stacji roboczych, d) Nielimitowanej ilości użytkowników M365, e) Nielimitowanej ilości repozytoriów GIT, f) Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu 2. Wsparcie techniczne: a) Świadczone jest w języku polskim, bezpośrednio przez główną siedzibę producenta, b) Zapewnia dostęp do aktualizacji oprogramowania, c) Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego, d) Obowiązuje przez okres minimum 60 miesięcy,
9.	**Obsługa SOC (Security Operation Center)**	1. Dostawca odpowiedzialny jest za kompleksowe wdrożenie systemu backupowego, obejmujące konfigurację macierzy, instalację agentów oraz uruchomienie polityk bezpieczeństwa, 2. Zamawiający wymaga przedstawienia mu technicznego przedstawiciela producenta systemu backupowego, który będzie świadczył mu pomoc techniczną w przypadku potrzeby uruchomienia narzędzi disaster recovery przez 24h na dobę, 7 dni w tygodniu i 365 dni w roku, 3. Techniczny przedstawiciel producenta lub osoba go zastępująca jest częściowo odpowiedzialna za weryfikację logów backupowych i powinna zawiadomić zamawiającego o przypadkach błędnego wykonywania się kopii zapasowych, 4. Techniczny przedstawiciel producenta ma obowiązek poświęcenia zamawiającemu min. 2h miesięcznie na konfigurację i utrzymanie systemu backupowego, obejmujące minimum ustalanie polityk bezpieczeństwa dla nowych urządzeń/środowisk oraz testowanie możliwości odtworzenia środowisk, 5. Zamawiający na początku każdego miesiąca kalendarzowego otrzyma raport poprawności wykonywania kopii zapasowych oraz poprawności odtwarzania testowego kopii zapasowych a także raport pracy z technicznym przedstawicielem producenta, 6. Komunikacja powinna odbywać się w 100% w języku polskim, 7. Zamawiający powinien mieć możliwość skorzystania ze szkoleń przeprowadzanych przez producenta min. 1 raz na kwartał, 8. Usługa powinna być dostępna przez okres minimum 60 miesięcy.

Wymagane i oferowane parametry techniczne i cechy użytkowe macierzy

Lp.	Parametry/cechy	Wymagane	**Oferowane** *(wpisać „Tak" lub podać wartość bądź opisać)*
1.	Elementy montażowe w zestawie	TAK	
2.	Obudowa	Rack 1U	
3.	Procesor	min. 20 GHz (ilość procesorów x ilość rdzeni x taktowanie)	
4.	Zasilacz	Redundantne, 2x450 W	
5.	Pamięć RAM	min. 32GB DDR4	
6.	Typy i pojemność dysków	urządzenie powinno być wyposażone w min. 8 dysków SAS 8TB	
7.	Typ i pojemność dysku dodatkowego	osobny dysk SSD min. 480 GB z preinstalowanym systemem backupowym spełniającym wymogi softwarowe zgodnie z OPZ	
8.	Zabezpieczenie danych na macierzy	Urządzenie powinno posiadać już zainstalowane dyski oraz skonfigurowany RAID 5, 6 lub 10 i być gotowe do pracy zgodnie z pkt. 1 OPZ	
9.	Interfejsy sieciowe Ethernet	min. 2 szt 10Gb SFP+, min. 2 szt. 1Gb Ethernet oraz dodatkowy 1Gb Ethernet do zdalnego zarządzania	
10.	Gwarancja	Gwarancja NBD on-premise na min. 5 lat	
11.	Dodatkowo	Możliwość uruchomienia na niej środowiska produkcyjnego w razie wystąpienia awarii.	

UWAGA:
Wszystkie pozycje w kolumnie „Oferowane" muszą być wypełnione przez Wykonawcę. W pozycjach tych należy wpisać „Tak" – jeżeli właściwość/cecha jest zgodna (identyczna) z wymaganym przez Zamawiającego lub podać wartość bądź opisać – w przypadku, gdy jest inna niż wymagana.
Oferowane oprogramowanie musi posiadać właściwości/cechy nie gorsze niż wymagane przez Zamawiającego.
Niespełnienie przez oferowane oprogramowanie któregokolwiek właściwości/cechy wymienionych w tabeli skutkować będzie odrzuceniem oferty. Jeżeli jakakolwiek pozycja nie zostanie wypełniona, Zamawiający uzna, że oferowane oprogramowanie nie spełnia wymogów określonych przez Zamawiającego i skutkować to będzie również odrzuceniem oferty.

Producent oprogramowania: …… *(wpisać)*

Nazwa: …… *(wpisać)*

Kalkulacja ceny

Lp.	Nazwa art.	j.m.	Ilość	Cena jedn. netto	Wartość netto [kol. 4 x kol. 5]	VAT ….%	Wartość brutto [kol. 6 + kol. 7]
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1.	Oprogramowanie do wykonywania kopii zapasowych wraz gotową macierzą	kpl.	**1**				
Razem netto, VAT, brutto *Kwoty należy przenieść do Formularza oferty pkt 4.3. Część 1*							

Miejscowość, data ……

Część 2. Dostawa serwera wraz z oprogramowaniem serwerowym – 1 kpl.

Wymagane i oferowane parametry techniczne i cechy użytkowe

Lp.	Parametry/cechy	Wymagania minimalne	Oferowane *(wpisać „Tak" lub podać wartość bądź opisać)*
1.	Obudowa	Obudowa o wysokości maksymalnie 1U dedykowana do zamontowania w szafie rack 19" z zestawem montażowym do szafy. Możliwość opcjonalnego doposażenia serwera w ramię kablowe. Minimum 12 zatok hot-swap, każda z możliwością skonfigurowania do użycia z dyskami SAS/SATA/NVMe	
2.	Procesor	Zainstalowany jeden procesor nie mniej niż, umożliwiające osiągnięcie w testach SPECrate2017_int_base wyniku nie mniejszego niż 218 punktów. Wynik testu dla platformy na której bazuje oferowany serwer muszą być opublikowane stronie spec.org	
3.	Pamięć RAM	Minimum 256GB DDR4 ECC Registered 3200MHz równomiernie rozłożone na wszystkich kanałach procesora. Serwer powinien posiadać wolne złącza w celu podwojenia ilości pamięci z zachowaniem zasady jej równomiernego rozłożenia na wszystkich kanałach	
4.	Płyta główna	Jednoprocesorowa, dedykowana do pracy w serwerach	
5.	Złącza rozszerzeń	Minimum jedno wolne (pod dalszą rozbudowę) złącze o przepustowości PCIe 4.0 x16	
6.	Karta sieciowa	Minimum dwa porty 1000BASE-T oraz dwa porty 10GBASE-T	
7.	Przestrzeń dyskowa	Zainstalowany sprzętowy kontroler SAS 12G z obsługą RAID 0,1,5,6,10,50,60 z 2GB pamięci cache zabezpieczonej przed utratą zasilania obsługujący nie mniej niż 8 zatok Zainstalowane osiem dysków SSD SATA Enterprise o żywotności 3DWPD i pojemności 960GB każdy. Dyski mają być podłączone do kontrolera RAID. Zainstalowane cztery dyski NVMe U.2 960GB o żywotności 1DWPD. Wolne złącze PCIe x4 na dysk NVMe M.2 22110	
8.	Karta graficzna	Zintegrowana z układem zarządzającym karta graficzna wyposażona w port VGA	
9.	USB i TPM	Nie mniej niż 2 porty USB 3.0. Zainstalowany moduł TPM 2.0	
10.	Zasilanie	Dwa redundantne zasilacze Hot-Plug, każdy o mocy minimum 650W i posiadające certyfikat efektywności energetycznej 80PLUS Platinum	
11.	Zarządzanie	Serwer musi być wyposażony w moduł zdalnego zarządzania (konsoli) pozwalający na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera, możliwość sprawdzenia aktualnego poziomu pobieranej energii, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu systemu operacyjnego). Funkcjonalność przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów bez konieczności dokładania dodatkowych kart sprzętowych. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną i z dedykowanym portem RJ45 niezależnym od wymaganych w serwerze kart sieciowych. Przekierowanie konsoli KVM oraz napędów musi wspierać HTML5 i nie może wymagać do działania technologii Java. Wsparcie dla Redfish.	
12.	Wymagania dodatkowe i certyfikaty	Zgodność z Windows Server 2019, RHEL8 / RHEL7, SLES 15, VMware ESXi. Deklaracja CE. Certyfikaty ISO 9001, ISO 14001 dla producenta sprzętu lub równoważny certyfikat jakości. Dostęp do strony internetowej producenta oferowanego sprzętu, a także prawo do pobierania / instalacji aktualizacji, sterowników, poprawek, uaktualnień oprogramowania układowego (firmware), bez dodatkowych opłat dla Zamawiającego; Zamawiający zastrzega sobie prawo do dokonywania rozbudowy sprzętu wynikających z nowych potrzeb (obudowa bez plomb). Możliwość sprawdzenia konfiguracji oraz warunków gwarancji oferowanego sprzętu na stronie producenta po podaniu numeru seryjnego. Zamawiający musi mieć możliwość dokonywania zgłoszeń poprzez: a) wyznaczone autoryzowane, polskojęzyczne punkty serwisowe producenta oraz serwis telefoniczny producenta, pracujący co najmniej w godzinach 9:00-16:00 we wszystkie dni robocze, bezpłatnie lub w cenie połączenia lokalnego w całej Polsce b) stronę WWW producenta w języku polskim zapewniającą przyjmowanie zgłoszeń serwisowych, c) zgłoszenie jak i obsługa zgłoszenia realizowana będzie w języku polskim	
13.	Gwarancja	3 lata gwarancji oraz serwisu realizowanego przez producenta serwera w następnym dniu roboczym w miejscu instalacji.	
14.	Oprogramowanie	Licencja Windows Server standard 2022 zgodne z licencjonowaniem Microsoft dla ilości CPU, Licencja dla systemu Windows Server standard 2022 CAL USER, Licencja dla system Windows Server standard 2022 dla połączenia Windows Remote Desktop Server User CAL	

UWAGA:
Wszystkie pozycje w kolumnie „Oferowane" muszą być wypełnione przez Wykonawcę. W pozycjach tych należy wpisać „Tak" – jeżeli parametr/cecha jest zgodny/-a (identyczny/-a) z wymaganym przez Zamawiającego lub podać wartość bądź opisać – w przypadku, gdy jest inny/-a niż wymagany/-a.
Oferowane urządzenie musi posiadać parametry techniczne lub cechy użytkowe nie gorsze niż wymagane przez Zamawiającego.
Niespełnienie przez oferowane urządzenie któregokolwiek parametru lub cechy wymienionych w tabeli skutkować będzie odrzuceniem oferty. Jeżeli jakakolwiek pozycja nie zostanie wypełniona, Zamawiający uzna, że oferowane urządzenie nie spełnia wymogów określonych przez Zamawiającego i skutkować to będzie również odrzuceniem oferty.

Producent urządzenia: …… *(wpisać)*

Nazwa i typ: …… *(wpisać)*

Kalkulacja ceny

Lp.	**Nazwa art.**	**j.m.**	**Ilość**	**Cena jedn. netto**	**Wartość netto** [kol. 4 x kol. 5]	**VAT ….%**	**Wartość brutto** [kol. 6 + kol. 7]
1	***2***	***3***	***4***	***5***	***6***	***7***	***8***
1.	Serwer	szt.	**1**				
2.	Licencja Windows Server standard 2022 x64 zgodne z licencjonowaniem Microsoft dla ilości CPU	szt.	**1**				
3.	Licencja dla systemu Windows Server standard 2022 CAL USER	szt.	**100**				
4.	Licencja dla system Windows Server standard 2022 dla połączenia Windows Remote Desktop Server User CAL	szt.	**5**				
Razem netto, VAT, brutto *Kwoty należy przenieść do Formularza oferty pkt 4.3. Część 2*							

Miejscowość, data ……

Część 3. Dostawa urządzenia klasy UTM oraz oprogramowania podnoszące bezpieczeństwo sieci komputerowej

Wymagane i oferowane parametry techniczne i cechy użytkowe urządzenia klasy UTM

Parametr	Charakterystyka
	1szt.
Elementy systemu bezpieczeństwa	• Urządzenia muszą mieć możliwość jednoczesnej pracy w trybie Layer 3 (routing), transparentnym (most) i Layer 2 (port mirroring) bez konieczności wirtualizacji sprzętu • System pełniący funkcję zapory musi mieć co najmniej 8 interfejsów Ethernet 10/100/1000 • Możliwość stworzenia minimum 128 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q. • W zakresie Firewall, obsługa nie mniej niż 1 000 000 jednoczesnych połączeń i 48 000 nowych połączeń na sekundę. • System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o minimalnej pojemności 8 GB do celów logowania i raportowania. • Możliwość rozszerzenia pamięci do 256GB poprzez dodatkowy dysk SSD bez otwierania obudowy urządzenia • Musi posiadać 2x USB 3.0 z przodu urządzenia • System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu. • Systemy wirtualne muszą obsługiwać QOS
Funkcjonalności	• Kontrola dostępu — zapora sieciowa Stateful Inspection • Ochrona przed wirusami - komercyjny antywirus [AV] • Poufność danych - IPSec VPN i SSL VPN • Kontrola witryn sieci Web — filtr URL • Kontrola zawartości poczty - antyspam (dla protokołów SMTP, POP3) • Kontrola przepustowości i ruchu [QoS i kształtowanie ruchu] z alokacją Tunnel w oparciu o strefę bezpieczeństwa, interfejs, adres, użytkownika/grupę użytkowników, serwera/ grupę serwerów, aplikację/grupę aplikacji, TOS, VLAN • Kontrola aplikacji i rozpoznawanie ruchu P2P (wideo, gry itp.) oraz ograniczanie nowych połączeń i jednoczesnych sesji • Reputacja IP • Cloud Sandbox
Wydajność	• Analiza ruchu szyfrowanego protokołem SSL • Wydajność Firewall co najmniej 5 Gb/s • Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym IPS i kontrolą aplikacji 1,2 Gb/s • Wydajność ochrony przed atakami (IPS) minimum 3.7 Gb/s • Ilość nowych sesji minimum 45 000

Funkcjonalności VPN	• Wydajność IPSec VPN, nie mniej niż 2,5 Gb/s • Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja • Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem. • Monitorowanie stanu tuneli VPN i utrzymywanie ich aktywności • Praca w toplogiach Hub and Spoke i Mesh • Wspierane mechanizamy : IPSec NAT Traversal, DPD, Replay Detection, Xauth, DHCP over IPsec, • Wsparcie grup DH dla IKEv1: 1,2,5,19,20,21,24 • Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,19,20,21,24 • Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance) • Obsługa PnPVPN (Plug and Play VPN)
Routing	• Rozwiązanie musi zapewniać: obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP, IS-IS • Obsługa Policy Based Routing • Funkcjonalność Virtual Wire
Translacja adresów NAT	• Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego. • Obsługa NAT46, NAT64, DNS64 • Wsparcie dla STUN
Polityka bezpieczeństwa systemu	• Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje bezpieczeństwa, rejestrowanie zdarzeń i zarządzanie pasmem sieci (w tym gwarantowaną i maksymalną przepustowość, priorytety). • Możliwosc budowania min. 8000 poliyk • Musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego • Musi być w stanie skonfigurować agregowane polityki • Musi być w stanie ograniczyć sesje na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu aplikacji (mysql, ms-sql, sqlnet, pobieranie P2P)
Wydzielenie stref bezpieczeństwa	• Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN • Musi mieć możliwosc konfiguracji oddzielnych wirtualnych routerów • Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników
Ochrona antywirusowa	• Silnik antywirusowy musi by ć oparty na przepływie tzw. flow-based • Musi umożliwiać skanowanie protokołów HTTP, SMTP, POP3, IMAP, FTP / SFTP, SMB • Możliwosc ręcznego dodawania lub usuwania sygantury MD5 do bazy danych AV • Musi obsługiwać wykrywanie wirusów w plikach skompresowanych, takich jak RAR, ZIP, GZIP, BZIP2, TAR, a także wykrywać wielowarstwowe pliki skompresowane dla nie mniej niż 5 warstw dekompresji

Rownoważenie obciążenia	• Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łącza dla określonej nazwy domeny oraz monitorowanie stanu łącza poprzez aktywną metodę wykrywania • Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted least-connection i weighted round-robin • Kontrola stanu serwera, monitorowanie sesji i ochrona sesji
Ochrona IPS	• Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury. • Baza danych wykrytych ataków musi zawierać co najmniej 12000 sygnatur. Dodatkowo musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i Ddos. • Funkcjonalnosc zapobiegania atakom SQL injection, XSS injection • Możliwość budowania własnych niestandardowych reguł IPS
Obrona przed atakiem	• Ochrona przed nieprawidłowym działaniem protokołu • Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment itp. • Wsparcie IPv4 jak i IPv6 dla o chrony przed DNS query flood i DNS reply flood • Biała listę docelowych adresów IP
Kontrola aplikacji	• Kontrola aplikacji musi być w stanie kontrolować ruch w oparciu o głęboką analizę pakietów, a nie tylko w oparciu o wartości portów TCP/UDP. • Baza danych aplikacji zawierająca ponad 4700 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka
Filtr adresów URL	• Baza filtrów URL pogrupowana w co najmniej 64 kategorie tematyczne. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków. • Możliwość zdefiniowania własnej bazy kategorii www. • Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL. • Kategoria takie jak hazard, malware, spam, botnety • Obsługa Safe Search • Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne • Dostosowanie strony ostrzeżenia
Ochrona danych	• Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy • Identyfikacja protokołu pliku, w tym HTTP、FTP、SMTP, POP3、IMAP • Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS • Filtrowanie plików przesyłanych przez SMB
Reputacja IP	• Identyfikuja i filtrowanie ruchu z ryzykownych adresów IP, takich jak hosty botnet, spamerzy, węzły Tor, podejrzane hosty i adresy IP atakujące metodą brute force • Logowanie, odrzucanie pakietów lub blokowanie dla różnych rodzajów ryzykownego ruchu IP

Zapobieganie botnetom	• Wykrywanie intranetowych hostó botnetu, monitorując połączenia C&C i blokowanie dalszych zaawansowanych zagrożeń takich jak botnet i oprogramowanie ransomware • Wsparcie DNS sinkhole • Wsparcie wykrywania tunelowania DNS • Wyrywanie i blokowanie DGA
Cloud Sandbox	• Złośliwe oprogramowanie emulowane w wirtualnym środowisku oparte na architekturze chmury w ceu wykrywania nieznanych zagrożeń • Obsługa protokołów, takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB • Obsługa typów plików : PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów • Obsługa blokowania wyników wykrywania w celu szybkiego blokowania nieznanych zagrożeń.
Uwierzytelnianie użytkownika	• System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika z nie mniej niż: o Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu o Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP o Hasła dynamiczne (RADIUS) oparte o zewnętrzne bazach danych o Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA • Musi umożliwiać budowę architektury uwierzytelniania pojedynczego logowania w środowisku Active Directory • Wsparcie usług terminalowych • Uwierzytelnianie użytkownika przez Web przed dotępem do internetu • Obsługa dwuskładnikowego uwierzytelniania, SMSy, certyfikaty i tokeny
Raportowanie i przeglądanie logów	• Wbudowany w system bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie • W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż: o Posiadanie predefiniowanych raportów dla ruchu internetowego, modułu IPS, skanera antywirusowego i antyspamowego o Generowanie co najmniej 10 rodzajów raportów
System logowania	• Wraz z systemem musi być zapewniony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy chmurowej, do której dostęp jest cały czas z dowolnego urządzenia oraz dedykowanej aplikacji mobilnej.
Certyfikaty	Rozwiązanie musi: • posiadać certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSA Labs dla funkcji Firewall • być pozycjonowanym w raporcie Gartnera przez ostatnie 7 lat

Zarządzanie	• Elementy systemu muszą mieć możliwość zarządzania lokalnie (HTTPS, SSH) oraz współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja między systemami bezpieczeństwa a platformami zarządzania musi odbywać się za pomocą protokołów szyfrowanych. • Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI bez instalowania oddzielnego oprogramowania, takiego jak dedykowana konsola
Gwarancja	Dostawa musi zawierać również: • Minimalną 60-miesięczną gwarancję producenta na dostarczone elementy systemu • Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 60 miesięcy • Wsparcie techniczne w języku polskim dystrybutora oferowanego rozwiązania • Szkolenie dla Administratora z oferowanego rozwiązania przeprowadzone przez dystrybutora oferowanego rozwiązania • Wdrożenie zdalne oferowanego rozwiązania przeprowadzone przez certyfikowanego inżyniera

Wymagane i oferowane funkcje oprogramowania

Lp.	Temat	Wymagane funkcje oprogramowania
1.	**Konsola zarządzająca**	1. Konsola web administratora powinna znajdować się w chmurze producenta znajdującej się na terenie Unii Europejskiej i zapewniać możliwość pełnego zarządzania stacjami roboczymi/serwerami przez przeglądarkę Web, która ma dostęp do Internetu, 2. Konsola web administratora musi posiadać możliwość wyboru języka polskiego, jako język całego interfejsu, 3. Konsola web musi umożliwiać zarządzanie stacjami roboczymi oraz serwerami i urządzeniami mobilnymi poprzez tą samą konsolę zarządzającą, 4. Konsola web musi posiadać możliwość tworzenia grup i polityk dla stacji, 5. Administrator musi mieć możliwość przeniesienia z poziomu konsoli aktywnej licencji na inną stację roboczą, urządzenia mobilne, bądź serwer bez utraty ważności licencji, 6. Administrator musi mieć możliwość zarządzania kluczem licencyjnym z poziomu konsoli administracyjnej, 7. Konsola web musi umożliwiać bezpieczne logowanie do konsoli zarządzającej po protokole HTTPS z certyfikatem, 8. Konsola web musi umożliwiać dwuetapową autoryzację logowania na minimum 2 sposoby, 9. Konsola web musi posiadać możliwość zablokowania dostępu do ustawień programu ochrony dla użytkowników na urządzeniach nieposiadających uprawnień administracyjnych, 10. Konsola web musi posiadać funkcję, która uniemożliwia użytkownikowi komputera wyłączenie działania monitora antywirusowego i innych składników ochrony, jeżeli nie posiada uprawnień administratora, 11. Konsola web musi posiadać narzędzie do wykonania instalacji oprogramowania na stacjach poprzez Active Directory, grupy robocze lub zakresy adresów sieciowych IP, 12. Konsola web musi umożliwiać wykonanie instalacji oprogramowania firm trzecich zdalnie z konsoli na stacjach, 13. Konsola web musi umożliwiać geolokalizację z aktualną mapą urządzeń mobilnych iOS/Android wyposażonych w moduł GPS, 14. Konsola web musi mieć możliwość zdefiniowana zalecanych aplikacji, które może pobrać użytkownik urządzeń mobilnych, 15. Konsola web umożliwia usuwanie aplikacji z urządzeń mobilnych, 16. Konsola web musi umożliwiać wyczyszczenie lub zablokowanie zdalne urządzenia mobilnego, 17. Konsola web musi mieć możliwość zalogowania się kilku administratorom jednocześnie, 18. Konsola web powinna oferować predefiniowane domyślne ustawienia rekomendowanych polityk (ustawień) dla stacji końcowych, 19. Konsola web musi mieć funkcję planowania zadań, w tym planowania terminów automatycznego skanowania, 20. Konsola web umożliwia zmianę ustawień priorytetu skanowania, 21. Konsola web umożliwia wysyłanie powiadomień o zdarzeniach na wskazany adres mailowy. 22. Konsola web musi posiadać możliwość uruchamiania komputerów zdalnie (WakaOnLAN), uruchamiania ponownego oraz wyłączania urządzeń z systemem Windows, 23. Konsola web musi umożliwiać synchronizację z Azure Active Directory, 24. Konsola web musi obsługiwać moduł do odbierania zgłoszeń serwisowych od użytkowników bezpośrednio z stacji klienckiej, 25. Rozwiązanie musi posiadać dedykowanego aplikację lub stronę internetową do zgłoszeń serwisowych bez konieczności instalacji ochrony antywirusowej, 26. Konsola web musi posiadać zintegrowany moduł CRM z możliwością zaplanowania prac u użytkownika, 27. Konsola web musi posiadać moduł uruchamiania procedur (skrypty) zdefiniowanych przez producenta

		oraz przez użytkownika w języku Python,
2.	**Zarządzanie aktualizacjami**	1. Oprogramowanie web musi zawierać zintegrowaną funkcjonalność menadżera aktualizacji (Patch Manager), który umożliwia zarządzanie pobieraniem aktualizacji (updatów) systemu Windows, Java, Adobe i innych producentów trzecich. 2. Producent powinien posiadać własne bezpieczne i sprawdzone repozytorium aplikacji do celów aktualizacji oprogramowania firm trzecich minimum 50 producentów.
3.	**Zarządzanie użytkownikami i stacjami**	1. Rozwiązanie musi umożliwiać bezpośrednio z konsoli zarządzającej web uruchamianie procedur (skryptów) serwisowych na stacjach klienckich o minimalnych, następujących funkcjonalnościach: a) Czyszczenie plików tymczasowych, b) Czyszczenie i sprawdzanie dysku, c) Usuwanie błędów dysku, d) Defragmentowanie dysku, e) Czyszczenie kolejki drukarki, f) Czyszczenie pamięci podręcznej DNS, g) Czyszczenie kosza, h) Sprawdzanie błędów na dysku twardym S.M.A.R.T. Check, i) Włączenie szyfrowania dysku funkcją Bitlocker dla systemu Windows, 2. System powinien przyjmować zgłoszenia serwisowe bezpośrednio z agenta na stacji, pocztą email oraz po przez dedykowaną stronę dla działu serwisu, 3. System musi umożliwiać przydzielanie zgłoszenia serwisowego dla konkretnego administratora oraz powinien mieć zintegrowany system diagnozy stacji oraz możliwość podłączenia się poprzez zdalny pulpit, 4. Konsola web musi posiadać zintegrowany moduł umożliwiający zdalne połączenie z graficznym pulpitem zdalnym przez dedykowaną aplikację dla komputerów/serwerów znajdujących się w sieci LAN i poza nią bez potrzeby tworzenia tuneli VPN każdej stacji komputera/serwera/Windows, 5. Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do użytkowania przez administratora w określonym przez niego czasie, 6. Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do użytkowania przez administratora w celu odpytania go o zgodę na połączenie, 7. Konsola web musi mieć funkcję tworzenia raportów o stacjach w konsoli, 8. Konsola web musi mieć funkcję logów wykonywanych czynności przez administratorów konsoli
4.	**Agent ochrony konsoli – oprogramowanie antywirusowe**	1. Program antywirusowy powinien mieć obsługę w języku polskim. Platforma powinna obsługiwać systemy operacyjne: a) Android: 4.x, 4.x (KNOX), 5.x, 5.x (KNOX), 6.x (KNOX), 7.x, 7.x (KNOX), 8.x, 8.x (KNOX), 9.x, 9.x (KNOX), 10.x, 10.x (KNOX), 11.x, 11.x (KNOX), 12.x, 12.x (KNOX), b) iOS: 7.x, 8.x, 9.x, 10.x, 11.x, 12.x, 13.x, 14.x, 15.x, c) macOS: 10.12.x, 10.13.x, 10.14.x, 10.15.x, 11.x, 12.x, d) Windows (workstation edition): Windows XP (SP3 or higher) x86, Windows 7 SP1 x86, Windows 7 SP1 x64, Windows 8 x86, Windows 8 x64, Windows 8.1 x86, Windows 8.1 x64, Windows 10 x86, Windows 10 x64, Windows 11 x64 e) Windows (wersja serwerowa): Windows Server 2003 SP2, Windows Server 2003 R2 SP2, Windows Server 2008 SP2, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, f) LinuxOS z gwarantowaną kompatybilnością: Latest Ubuntu 16.x LTS x64 release version (with GUI), Latest Ubuntu 18.x LTS x64 release version (with GUI), Latest Ubuntu 19.x x64 release version (with GUI), Latest Ubuntu 20.x LTS x64 release version (with GUI), Latest Ubuntu 21.04 x64 release version (with GUI), Latest Debian 8.x x64 release version (with GUI), Latest Debian 9.x x64 release version (with GUI), Latest Debian 10.x x64 release version (with GUI), Latest Red Hat Enterprise Linux Server 7.x x64 release version (with GUI), Latest Red Hat Enterprise Linux Server 8.x x64 release version (with GUI), Latest CentOS 7.x x64 release version (with GUI), Latest CentOS 8.x x64 release version (with GUI), 2. Rozwiązanie powinno działać na komputerach wyposażonych minimalnie w: 512 MB dostępnej pamięci RAM, 1 GB miejsca na dysku twardym dla wersji 32-bitowej i 64-bitowej, 3. Instalacja oprogramowania musi być możliwa poprzez Active Directory, grupy robocze, poprzez sieć, pobranie paczki MSI i za pomocą dystrybucji przez pocztę e-mail, 4. Ochrona poczty - antywirus musi chronić stacje poprzez uruchamianie nieznanych oraz niebezpiecznych załączników w środowisku wirtualnym na stacji takim jak lokalna i automatyczna piaskownica (auto-sandbox), 5. Program antywirusowy musi posiadać możliwość skanowania wybranych plików, folderów/katalogów (również skompresowanych), a także całych dysków (w tym sieciowych) czy partycji, 6. Program antywirusowy musi posiadać możliwość skanowania dowolnego zasobu podłączonego do stacji roboczej np.: dyski zewnętrzne, pamięci USB, 7. Program antywirusowy powinien posiadać filtering URL umożliwiający blokowanie konkretnych stron internetowych, 8. Program antywirusowy musi posiadać moduł antywirusowy chroniący w czasie rzeczywistym, 9. Program antywirusowy musi posiadać moduł sprawdzający reputację plików w chmurze, 10. Program antywirusowy musi posiadać dwukierunkowy konfigurowalny z konsoli web firewall z możliwością tworzenia polityk globalnych i z podziałem na aplikacje, 11. Program antywirusowy musi posiadać moduł HIPS (Host Intrusion Protection System – ochrona antywłamaniowa), 12. Program antywirusowy musi posiadać moduł automatycznej piaskownicy (autosandbox), odizolowanego środowiska wirtualnego, w którym zasoby są emulowane dla obiektów w nim umieszczonych. Dodatkowo cały proces izolacji dzięki temu modułowi musi odbywać się lokalnie, na stacji roboczej. Całe środowisko wirtualne musi być odwzorowaniem 1:1 z systemem operacyjnym. Użytkownik powinien móc pracować w zwirtualizowanym środowisku, bez możliwości zapisu na stacji poza środowiskiem wirtualnym, 13. Program antywirusowy musi posiadać możliwość uruchomienia dowolnego pliku/programu w automatycznej piaskownicy (auto-sandbox) na żądanie użytkownika (manualnie), 14. Program antywirusowy musi umożliwiać użytkownikowi wysłanie podejrzanego obiektu do producenta oprogramowania antywirusowego w celu jego analizy. Funkcja ta powinna być dostępna z interfejsu

		programu antywirusowego, 15. Podczas pracy komputera Program musi automatycznie skanować: a) pliki uruchamiane, otwierane, b) pliki kopiowane lub przenoszone, c) pliki tworzone, d) pliki pobierane z Internetu po protokole HTTP/HTTPS, 16. W przypadku wykrycia wirusa program musi posiadać możliwość automatycznego poddawania kwarantannie podejrzanych obiektów oraz opcję przywrócenia z kwarantanny usuniętych obiektów, 17. Program antywirusowy musi posiadać funkcję dodawania wyjątków do modułu antywirusowego, automatycznej piaskownicy (auto-sandbox) czy modułu HIPS, 18. Program antywirusowy powinien posiadać dodatkowe narzędzie do skanowania systemu, 19. Program antywirusowy musi posiadać dodatkowe narzędzie do analizowania bezpieczeństwa procesów, 20. Program antywirusowy powinien mieć możliwość skanowania skompresowanych plików, 21. Program antywirusowy musi być z możliwością zablokowania dostępu do zmiany ustawień programu hasłem administratora oraz hasłem skonfigurowanym w konsoli zarządzającej, 22. Program antywirusowy powinien mieć możliwość importowania oraz eksportowania ustawień, 23. Program antywirusowy powinien mieć możliwość tworzenia list zaufanych procesów, 24. Program antywirusowy powinien mieć możliwość tworzenia list zaufanych plików, 25. Program antywirusowy i konsola powinny umożliwiać tworzenie wyjątków ze skanowania folderów / plików, 26. Program antywirusowy powinien umożliwiać konfigurację polityk (globalnych ustawień dla grup endpoint'ów) w celu szybkiej implementacji ustawień bezpieczeństwa dla wielu urządzeń, 27. Program antywirusowy powinien umożliwiać zmianę ustawień priorytetu skanowania, 28. Program antywirusowy powinien umożliwiać skanowanie pamięci komputera po uruchomieniu, 29. Program antywirusowy posiada zintegrowaną funkcję skanowania plików pod kątem danych wrażliwych (DLP), 30. Program antywirusowy posiada zintegrowaną funkcję blokowania urządzeń zewnętrznych / przenośnych przed odczytem, edycją i zapisem plików w tym samym czasie, 31. Program antywirusowy posiada zintegrowaną funkcję blokowania jedynie zapisu plików na urządzeniach zewnętrznych / przenośnych, 32. Program antywirusowy powinien posiadać możliwość aktualizowania baz danych antywirusowych ręcznie, nawet jeśli komputer nie będzie miał dostępu do Internetu, 33. Program antywirusowy musi posiadać zintegrowane środowisko, dzięki któremu możemy bezpiecznie działać w wirtualnym systemie nawet na zainfekowanej stacji. Środowisko to musi być odizolowanie od reszty systemu operacyjnego i mieć możliwość uruchomienia takich sesji bez wprowadzonych wcześniejszych zmian przez użytkownika w tym narzędziu (czyste środowisko). Ma również pozwalać na bezpieczniejsze wykonywanie przelewów bankowych, bez obaw, że system operacyjny, na którym działa dany komputer nie został uprzednio zmodyfikowany i byłby w stanie zagrozić utracie np. danych logowania do kont bankowych, 34. Oprogramowanie powinno mieć możliwość przeglądania obciążenia procesów na stacji i serwerze oraz zawartości dysków z poziomu konsoli web,
5.	**Dodatkowe systemy bezpieczeństwa**	1. Konsola web musi posiadać możliwość śledzenia historii zagrożeń na wybranych komputerach, 2. Konsola web musi posiadać moduł zapobiegania wyciekowi danych DLP z możliwością włączenia skanowania plików w wybranych lokalizacjach na komputerach pod kątem znajdujących się w nich danych wrażliwych przez zdefiniowane wzory z możliwością dodawania własnych reguł DLP oraz powinna umożliwiać sprawdzenia logów z tej czynności, 3. Konsola web zintegrowana z wszystkimi poprzednimi modułami i funkcjami musi umożliwić przeprowadzenia skanowania sieci firmowej (również za pomocą protokołu SNMP) w celu przeprowadzenia audytu urządzeń działających w tej sieci.

Kalkulacja ceny

Lp.	**Nazwa art.**	**j.m.**	**Ilość**	**Cena jedn. netto**	**Wartość netto** [kol. 4 x kol. 5]	**VAT ….%**	**Wartość brutto** [kol. 6 + kol. 7]
1	***2***	***3***	***4***	***5***	***6***	***7***	***8***
1.	Urządzenie klasy UTM	szt.	**1**				
2.	Oprogramowanie podnoszące bezpieczeństwo sieci	szt.	**1**				
Razem netto, VAT, brutto *Kwoty należy przenieść do Formularza oferty pkt 4.3. Część 3*							

Miejscowość, data ……

Elektronicznie podpisany przez Ewa Nakiewicz