Załącznik nr 1 do SWZ

Opis przedmiotu zamówienia

Część I - Dostawa sprzętu i oprogramowania na potrzeby Urzędu Gminy Popów

	Nazwa	**Opis**	**Ilość**	**Parametry oferowanego sprzętu**
1.	Notebook	**Typ:** Komputer typu notebook z ekranem o przekątnej 15'6 cala i rozdzielczości nie mniejszej niż 1920 x 1080 pikseli (FullHD). Podświetlenie LED, matryca wykonana w technologii IPS lub EWV/VA. Jasność matrycy nie mniejsza niż 250 nitów. Kontrast nie mniejszy niż 700:1. Matryca z fabryczną powłoką przeciwodblaskową. Pokrywa matrycy wykonana z aluminium lub innego metalu w celu dodatkowego zabezpieczenia panelu LCD. **Procesor:** Procesor klasy x86, o min. 4 rdzeniach fizycznych i 8 wątkach logicznych, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem, co najmniej 2,40 GHz, z pamięcią cache co najmniej 8 MB, osiągający jednocześnie w teście PassMark Performance Test, co najmniej 10000 punktów w kategorii Average CPU Mark (wynik na dzień publikacji SWZ) i po raz pierwszy będący na wykresach PassMark „CPU First Seen on Charts" w latach 2020-2021. **Pamięć RAM:** DDR4 8 GB z możliwością rozbudowy do min. 32 GB z pełnym wsparciem dla pamięci działających z taktowaniem 3200MHz. 1 wolny bank pamięci pozwalający na dalszą rozbudowę. Pamięć operacyjna/magazyn danych M.2 PCIe 256GB o parametrach odczyt/zapis 1200/1200MB/s. Możliwość dołożenia drugiego dysku pracującego w standardzie SATA lub NVMe bez utraty gwarancji. **Karta graficzna:** Grafika zintegrowana z procesorem ze sprzętowym wsparciem dla kodowania H.264 oraz MPEG2, DirectX 12.1, OpenGL 4.6, posiadająca minimum 80 jednostek wykonawczych. **Multimedia:** Karta dźwiękowa zgodna z HD Audio. Wbudowane głośniki. Kamera HD. Łączność Karta WLAN 802.11ax (Wifi6) + BlueTooth 5.2. Zintegrowana gigabitowa karta LAN – zamawiający nie dopuszcza możliwości zastosowania karty USB-LAN. **Bateria i zasilacz:** Minimum 3 komorowa o pojemności 42Wh. Zasilacz dedykowany do notebooka - brandowany logo Producenta komputera. **Funkcje BIOS:**	1 szt.	

		BIOS zgodny ze specyfikacją UEFI. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS bieżących informacji o: - numerze seryjnym komputera. - wersji BIOS. - ilości zainstalowanej pamięci RAM. - zastosowanym procesorze wraz z taktowaniem. - zamontowanym dysku twardym wraz z jego pojemnością i modelem.. Możliwość włączenia/wyłączenia zintegrowanego z komputerem touchpada. Możliwość włączenia/wyłączenia technologii Hyper-Threading. Możliwość włączenia/wyłączenia wirtualizacji. Możliwość włączenia/wyłączenia VT-d (Virtualization Technology for Directed I/O). Możliwość włączenia/wyłączenia testu SMART zamontowanego dysku. Możliwość włączenia/wyłączenia bezprzewodowej karty sieciowej i modułu BlueTooth. Możliwość włączenia/wyłączenia zintegrowanej karty LAN. Możliwość włączenia/wyłączenia karty dźwiękowej. Możliwość włączenia/wyłączenia zintegrowanej kamery. Możliwość włączenia/wyłączenia portów USB. Możliwość włączenia/wyłączenia modułu TPM. Możliwość ustawienia niezależnych haseł dla konta administratora, użytkownika i dysku twardego. Brak możliwości uruchomienia systemu operacyjnego bez podania hasła. Funkcja ustawień zależności między hasłem administratora a użytkownika tak, aby nie było możliwe wprowadzenie zmian z poziomu użytkownika bez podania hasła do konta administratora. Główne hasło zabezpieczające rozruch musi być zachowane nawet w przypadku odcięcia wszystkich źródeł zasilania (wliczając baterię RTC/CMOS). **Certyfikaty i standardy:** CE dla oferowanego komputera. Oferowany laptop musi spełniać wymagania normy MIL-STD-810H lub normy równoważnej. ISO 9001:2015 dla autoryzowanego serwisu Producenta notebooka. **Waga i wymiary:** Waga nieprzekraczająca 1,75kg, wymiary maksymalne 36x24x1,95cm Bezpieczeństwo: Dedykowana dioda LED zintegrowanej kamery sygnalizująca pracę komponentu. Fizyczna przesłona na kamerze zintegrowana z obudową komputera. Zintegrowany z płytą główną moduł TPM Zintegrowane z obudową gniazdo Kensington Wbudowany w obudowę czytnik linii papilarnych **Warunki gwarancji:** Minimum 36 miesięcy. Gwarancja realizowana na miejscu u klienta. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych. Wymagana gwarancja na baterię Gwarancja na baterię nie może być krótsza niż gwarancja na całe urządzenie. W przypadku oferty, w której notebook		

		posiada gwarancję 36 miesięcy, również bateria powinna być objęta takim samym czasem ochrony tj. 36 miesięcy. **Wsparcie techniczne producenta:** Możliwość sprawdzenia telefonicznego bezpośrednio u producenta oraz na stronie internetowej producenta oferowanego notebooka, po podaniu numeru seryjnego - konfiguracji sprzętowej notebooka oraz warunków gwarancji. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta notebooka, realizowany poprzez podanie na stronie internetowej producenta numeru seryjnego lub modelu notebooka Porty - 2 porty USB typ A (3.2 Gen 2) - 1 port USB typ A (2.0) - 1 port USB typ C z wsparciem dla ładowania notebooka i Displayport - 1 port HDMI - 1 port VGA - 1 port LAN RJ45 - 1 port czytnika MicroSD - 1 port audio 3.5mm jack (combo lub osobne łącza) **Klawiatura** Z dedykowanym blokiem numerycznym po prawej stronie, podświetlona. **System operacyjny** Windows 10 PRO lub równoważny		
2.	Notebook	**Typ:** Komputer typu notebook z ekranem o przekątnej 15'6 cala i rozdzielczości nie mniejszej niż 1920 x 1080 pikseli (FullHD). Podświetlenie LED, matryca wykonana w technologii IPS lub EWV/VA. Jasność matrycy nie mniejsza niż 250 nitów. Kontrast nie mniejszy niż 700:1. Matryca z fabryczną powłoką przeciwodblaskową. Pokrywa matrycy wykonana z aluminium lub innego metalu w celu dodatkowego zabezpieczenia panelu LCD. **Procesor:** Procesor klasy x86, o min. 2 rdzeniach fizycznych i 4 wątkach logicznych, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem, co najmniej 1,7 GHz, z pamięcią cache co najmniej 6 MB, osiągający jednocześnie w teście PassMark Performance Test, co najmniej 6200 punktów w kategorii Average CPU Mark (wynik na dzień publikacji SWZ) i po raz pierwszy będący na wykresach PassMark „CPU First Seen on Charts" w latach 2020-2021. **Pamięć RAM:** DDR4 8 GB z możliwością rozbudowy do min. 32 GB z pełnym wsparciem dla pamięci działających z taktowaniem 3200MHz. 1 wolny bank pamięci pozwalający na dalszą rozbudowę. Pamięć operacyjna/magazyn danych M.2 PCIe 256GB o parametrach odczyt/zapis 1200/1200MB/s. Możliwość dołożenia drugiego dysku pracującego w standardzie SATA lub NVMe bez utraty gwarancji. **Karta graficzna:** Grafika zintegrowana z procesorem ze sprzętowym wsparciem dla kodowania H.264 oraz MPEG2, DirectX 12.1, OpenGL 4.6, posiadająca minimum 48 jednostki wykonawcze. **Multimedia:** Karta dźwiękowa zgodna z HD Audio. Wbudowane głośniki. Kamera HD. **Łączność** Karta WLAN 802.11ax (Wifi6) + BlueTooth 5.2. Zintegrowana gigabitowa karta LAN – zamawiający nie dopuszcza możliwości zastosowania karty USB-LAN. **Bateria i zasilacz:** Minimum 3 komorowa o pojemności 42Wh. Zasilacz dedykowany do notebooka -brandowany logo Producenta komputera.	1 szt.	

		Funkcje BIOS: BIOS zgodny ze specyfikacją UEFI. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS bieżących informacji o: - numerze seryjnym komputera. - wersji BIOS. - ilości zainstalowanej pamięci RAM. - zastosowanym procesorze wraz z taktowaniem. - zamontowanym dysku twardym wraz z jego pojemnością i modelem.. Możliwość włączenia/wyłączenia zintegrowanego z komputerem touchpada. Możliwość włączenia/wyłączenia technologii Hyper-Threading. Możliwość włączenia/wyłączenia wirtualizacji. Możliwość włączenia/wyłączenia VT-d (Virtualization Technology for Directed I/O). Możliwość włączenia/wyłączenia testu SMART zamontowanego dysku. Możliwość włączenia/wyłączenia bezprzewodowej karty sieciowej i modułu BlueTooth. Możliwość włączenia/wyłączenia zintegrowanej karty LAN. Możliwość włączenia/wyłączenia karty dźwiękowej. Możliwość włączenia/wyłączenia zintegrowanej kamery. Możliwość włączenia/wyłączenia portów USB. Możliwość włączenia/wyłączenia modułu TPM. Możliwość ustawienia niezależnych haseł dla konta administratora, użytkownika i dysku twardego. Brak możliwości uruchomienia systemu operacyjnego bez podania hasła. Funkcja ustawień zależności między hasłem administratora a użytkownika tak, aby nie było możliwe wprowadzenie zmian z poziomu użytkownika bez podania hasła do konta administratora. Główne hasło zabezpieczające rozruch musi być zachowane nawet w przypadku odcięcia wszystkich źródeł zasilania (wliczając baterię RTC/CMOS). **Certyfikaty i standardy:** CE dla oferowanego komputera. Oferowany laptop musi spełniać wymagania normy MIL-STD-810H lub normy równoważnej. ISO 9001:2015 dla autoryzowanego serwisu Producenta notebooka. **Waga i wymiary:** Waga nieprzekraczająca 1,75kg, wymiary maksymalne 36x24x1,95cm **Bezpieczeństwo:** Dedykowana dioda LED zintegrowanej kamery sygnalizująca pracę komponentu. Fizyczna przesłona na kamerze zintegrowana z obudową komputera. Zintegrowany z płytą główną moduł TPM Zintegrowane z obudową gniazdo Kensington Wbudowany w obudowę czytnik linii papilarnych **Warunki gwarancji:** Minimum 36 miesięcy. Gwarancja realizowana na miejscu u klienta. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych. **Wymagana gwarancja na baterię:**		

		Gwarancja na baterię nie może być krótsza niż gwarancja na całe urządzenie. W przypadku oferty, w której notebook posiada gwarancję 36 miesięcy, również bateria powinna być objęta takim samym czasem ochrony tj. 36 miesięcy. **Wsparcie techniczne producenta:** Możliwość sprawdzenia telefonicznego bezpośrednio u producenta oraz na stronie internetowej producenta oferowanego notebooka, po podaniu numeru seryjnego - konfiguracji sprzętowej notebooka oraz warunków gwarancji. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta notebooka, realizowany poprzez podanie na stronie internetowej producenta numeru seryjnego lub modelu notebooka **Porty** - 2 porty USB typ A (3.2 Gen 2) - 1 port USB typ A (2.0) - 1 port USB typ C z wsparciem dla ładowania notebooka i Displayport - 1 port HDMI - 1 port VGA - 1 port LAN RJ45 - 1 port audio 3.5mm jack (combo lub osobne łącza) **Klawiatura** Z dedykowanym blokiem numerycznym po prawej stronie, podświetlona. **System operacyjny:** Windows 10 PRO lub równoważny		
3.	Komputer stacjonarny.	**Typ:** Komputer stacjonarny plus monitor. W ofercie wymagane jest podanie modelu, symbolu oraz nazwy producenta. **Procesor:** Wydajność obliczeniowa: Procesor taktowany zegarem co najmniej 3.6 GHz, 4 rdzeni oraz 8 wątków logicznych, w architekturze x64. Procesor powinien osiągać w teście wydajności PassMark PerformanceTest co najmniej wynik 8,788 punktów Passmark CPU Mark. Wynik zaproponowanego procesora musi znajdować się na stronie https://www.cpubenchmark.net/cpu_list.php ***Przed podpisaniem umowy Wykonawca, którego oferta zostanie najwyżej oceniona, przedłoży Zamawiającemu potwierdzony za zgodność z oryginałem wydruk poświadczający wynik procesora.*** **Pamięć operacyjna:** 1 x 8GB DDR4, możliwość rozbudowy do min 64GB, częstotliwość taktowania nie mniej niż 2666 MHz. **Parametry pamięci masowej:** 256GB SSD PCIe M.2 NVMe, **Karta graficzna:**Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem dla DirectX 12, OpenCL 2.0, OpenGL 4.4, HLSL shader model 5.1. **Wyposażenie multimedialne:**Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition 5.1, porty słuchawek i mikrofonu na tylnym panelu obudowy. **Obudowa:**Typu Small Form Factor Pobór mocy maksimum 200 W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 92%, przy 50-procentowym obciążeniu. Zasilacz wbudowany w obudowę.	9 szt.	

		<u>BIOS</u>: Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: • wersji BIOS, • ilości i sposobu obłożenia slotów pamięciami RAM, • typie procesora wraz z informacją o ilości rdzeni, pojemności zainstalowanego dysku twardego • rodzajach napędów optycznych • MAC adresie zintegrowanej karty sieciowej • kontrolerze audio Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS) Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora. Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowy tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. Możliwość wyłączania portów USB w tym: wszystkich portów, tylko portów znajdujących się na przedzie obudowy, tylko tylnych portów. **<u>Ergonomia:</u>** Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie jałowym (IDLE) wynosząca maksymalnie 18 dB (załączyć oświadczenie producenta wraz z raportem badawczym wystawionym przez akredytowaną jednostkę). Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż pamięci RAM i napędów bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych). Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej.		

		Wymagania dodatkowe: Zainstalowany system operacyjny równoważny z wzorcowym Microsoft Windows 11 Professional w języku polskim w wersji 64-bitowej, niewymagający aktywacji za pomocą telefonu lub Internetu. Oprogramowanie równoważne musi posiadać następujące cechy: - zgodność z Windows 11 API, możliwość uruchamiania oprogramowania przeznaczonego do pracy na platformie Windows zarówno 32 jak i 64 bitowego bez dodatkowego oprogramowania pośredniczącego, możliwość centralnego zarządzania systemem operacyjnym bez dodatkowego oprogramowania za pomocą usług katalogowych opartych na protokole LDAP kompatybilnych ze strukturą zarządzania opartą na serwerze domenowym Windows Server 2012; - możliwość instalacji systemu niewymagająca aktywacji za pomocą telefonu lub Internetu; - w przypadku dostarczenia oprogramowania równoważnego należy zapewnić szkolenie dla każdego użytkownika w wymiarze co najmniej 80 godzin na miejscu, w siedzibie Zamawiającego. **Wbudowane porty:** - 1 x VGA (15 pin D-Sub) - 1 x HDMI - 1 x RJ-45 10/100/1000 Mbit/s - 1 x Bluetooth - 1 x Audio: (Słuchawki / Line-out) - 1 x Audio: (Combo) - 8 x USB w tym: minimum 4x USB 3.0, 4x USB 2.0 Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego (TPM co najmniej w wersji 2.0). Klawiatura USB w układzie QWERTY US, 104 klawisze. Mysz laserowa USB z trzema klawiszami oraz rolką (scroll) min 800dpi. Nagrywarka DVD +/-RW. W zestawie kabel zasilający min 1,5m oraz kabel sieciowy RJ45 min 3m. Dostarczony sprzęt musi być fabrycznie nowy, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Wszystkie komponenty i podzespoły komputera muszą pochodzić od jednego producenta lub muszą być przez niego certyfikowane. *Wymagane oświadczenie Wykonawcy w druku oferta, że oferowany do przetargu sprzęt spełnia ten wymóg.* Wymaga się: 1. Dla potwierdzenia, że oferowany sprzęt odpowiada postawionym wymaganiom i był wykonany przez Wykonawcę (a jeżeli Wykonawca nie jest producentem to przez producenta) w systemie zapewnienia jakości wg normy ISO 9001, aby		

		Wykonawca posiadał: Certyfikat ISO 9001 lub inne zaświadczenie/dokument wydane przez niezależny podmiot zajmujący się poświadczaniem zgodności działań wykonawcy z normami jakościowymi -odpowiadającej normie ISO 9001. 2. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia wykonawcy wystawionego na podstawie dokumentacji producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram. 3. Gwarancji jakości producenta. *Przed podpisaniem umowy Wykonawca, którego oferta zostanie najwyżej oceniona, przedłoży Zamawiającemu, oświadczenie Wykonawcy, potwierdzające, że oferowany do przetargu sprzęt spełnia te wymagania.* **Gwarancja:** Komputer musi posiadać pakiet serwisowy oferujący następujące warunki gwarancji. 1. Gwarancja 36 miesięcy na części i robociznę. 2. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. **Monitor:** 24.00 cali Typ matrycy:IPS (In-Plane Switching) Format obrazu - 16:9 Czas reakcji matrycy - 5.0 ms Jasność matrycy - 250 cd/m2 Kontrast statyczny - 1000 :1 Rozdzielczość maksymalna - 1920 x 1080 (Full HD) Częst. odświeżania przy rozdzielczości optymalnej - 75 Hz **Aktywny obszar wyświetlania (Szer. x Wys.) (mm)** min: 527.04 × 296.46 mm Kąt widzenia pionowy (V) - 178.00 stopni Kąt widzenia poziomy (H) - 178.00 stopni Złącza - D-Sub / VGA, HDMI **Wyposażenie dodatkowe** Kabel zasilający, kabel HDMI. Płyta Instalacyjna Certyfikaty Eco Saving Plus, Tryb Eye Saver, Tryb Gry, Off Timer Plus; Certyfikacja Windows 10; HDMI 1.4.		

<table>
<tr>
<td></td>
<td></td>
<td>Regulacja kąta nachylenia -2° / +20°
Pobór energii (podczas pracy) - 25.00 W
Pobór energii (tryb czuwania) - 0.50 W
Kolor obudowy - Czarny (Black)
Wymiary z podstawą [S x W x G] (mm)- 539,2 x 425,3 x 232?
Montaż VESA- 100 x 100
Wbudowany zasilacz - Nie

Funkcje

<table>
<tr><td>Eco Saving Plus</td><td>Tak</td></tr>
<tr><td>Eye Saver Mode</td><td>Tak</td></tr>
<tr><td>Flicker Free</td><td>Tak</td></tr>
<tr><td>Game Mode</td><td>Tak</td></tr>
<tr><td>Image Size</td><td>Tak</td></tr>
<tr><td>Windows Certification</td><td>Windows 10</td></tr>
<tr><td>AMD FreeSync™</td><td>Tak</td></tr>
<tr><td>Off Timer Plus</td><td>Tak</td></tr>
</table>

Gwarancja : 24 miesiące</td>
<td>9 szt</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Serwer domenowy</td>
<td><u>Obudowa</u>
• Typu RACK, wysokość nie więcej niż 2U;
• Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
<u>Płyta główna</u>
• Dwuprocesorowa;
• Wyprodukowana i zaprojektowana przez producenta serwera
• 6 złącz PCI Express generacji 3 w tym:
○ 3 złącza o prędkości x16
○ 3 złącza o prędkości x8
• 12 gniazd pamięci RAM;
• Obsługa minimum 768GB pamięci RAM;
• Możliwość zainstalowania modułu TPM;</td>
<td>1 szt.</td>
<td></td>
</tr>
</table>

		• Wsparcie dla technologii: ○ Memory Scrubbing ○ SDDC ○ Advanced ECC **Procesory** • Dwa procesory 8-rdzeniowe • architektura x86_64 • Taktowanie bazowe 2,1GHz zapewniający wydajność min. 11110 pkt. (dla pojedynczego procesora) w teście Passmark CPU Mark, znajdujący się na liście https://www.cpubenchmark.net/cpu_list.php (wynik na dzień 29.04.2022) **Pamięć RAM** • 64 GB pamięci RAM • DDR4 Registered • 2933Mhz **Dyski twarde** • Minimum 8 wnęk dla dysków twardych Hotplug 3,5"; • Zainstalowane 2 dyski SSD SATA 480GB HOT PLUG 3.5" Mixed USE • Zainstalowane 4 dyski SATA 4TB HOT PLUG 3.5" **Kontrolery LAN** • Trwale zintegrowana karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 1Gbit Base-T ze wsparciem iSCSI i iSCSI boot; • Karta sieciowa 2x10Gbit SFP+ **Kontrolery I/O** • Możliwość zainstalowania dwóch nośników flash o pojemności 64GB w konfiguracji RAID-1, rozwiązanie dedykowane dla hypervisora oraz niezajmujące zatok dla dysków hot-plug • Kontroler RAID dla wewnętrznych dysków twardych posiadający obsługujący poziomy RAID: 0,1,10,5,50,6,60 posiadający 2GB pamięci cache zabezpieczonej przed utratą danych w przypadku awarii zasilania (FBU lub BBU)) **Porty** • Zintegrowana karta graficzna ze złączem VGA; • 2 porty USB 3.0 na panelu przednim; • 1 port USB 3.0 wewnętrzny; • 4 porty USB 3.0 dostępne z tyłu serwera; • 1 port serial/RS232 – możliwość rozbudowy; • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; **Zasilanie, chłodzenie** • Dwa zasilacze hotplug o sprawności 94% (tzw klasa Platinum) o mocy 450W, redundancja zasilania; • Redundantne wentylatory;		

		Zarządzanie • Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera; • Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: ○ Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; ○ Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; ○ Dostęp poprzez przeglądarkę Web, SSH; ○ Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; ○ Zarządzanie alarmami (zdarzenia poprzez SNMP) ○ Możliwość przejęcia konsoli tekstowej ○ Możliwość zarządzania przez 6 administratorów jednocześnie ○ Opcjonalne przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); ○ Obsługa serwerów proxy (autentykacja) ○ Obsługa VLAN ○ Możliwość konfiguracji parametru Max. Transmission Unit (MTU) ○ Wsparcie dla protokołu SSDP ○ Obsługa protokołów TLS 1.2, SSL v3 ○ Obsługa protokołu LDAP ○ Integracja z HP SIM ○ Synchronizacja czasu poprzez protokół NTP ○ Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); • Opcjonalna pamięć flash o pojemności minimum 16 GB (lub wbudowana w kartę zarządzającą); dająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; • Serwer posiada opcjonalnie możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. **Wspierane OS:** • Microsoft Windows Server 2019, 2016 • VMWare vSphere 6.7 • Suse Linux Enterprise Server 12 • Red Hat Enterprise Linux 7 **Gwarancja:** • 5 lat gwarancji producenta serwera w trybie onsite z gwarantowanym przyjazdem certyfikowanego przez producenta		

		pracownika serwisu do końca następnego dnia roboczego; ● Zgłaszanie usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu (bez udziału administratora) – opcja rozbudowy; ● Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; ● Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; ● Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty); **Dokumentacja, inne:** ● Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy; ● Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy; ● Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; ● W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.		

		6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o:		

		a. Login i hasło, b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: c. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, d. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, e. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. f. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. g. Zdalna dystrybucja oprogramowania na stacje robocze.		

		h. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej i. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: Dystrybucję certyfikatów poprzez http Konsolidację CA dla wielu lasów domeny, Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. Szyfrowanie plików i folderów. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. Serwis udostępniania stron WWW. Wsparcie dla protokołu IP w wersji 6 (IPv6), Wsparcie dla algorytmów Suite B (RFC 4869), Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: • Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, • Obsługi ramek typu jumbo frames dla maszyn wirtualnych. • Obsługi 4-KB sektorów dysków • Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra • Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. • Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)		

		• Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. • Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). • Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. • Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. • Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. • Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. **Dodatkowe licencje:** **Microsoft Oprogramowanie OEM Win Svr CAL 2019 PL User 1Clt – 32 szt** **Windows Server 2019 - 1 User CALs – 32 licencji (CAL'e per user dla 32 użytkowników dla Windows Server)** Opis wymagań (wymagania minimalne dla równoważnego oprogramowania): Licencje dla użytkownika typu CAL uprawniająca do korzystania z usług takich jak drukowanie sieciowe, przechowywanie plików w systemie Windows Server 2019 (ActiveDirectory). Zamówienie dotyczy licencji bezterminowych. Wymagany komplet koniecznych kluczy aktywacyjnych. Zamówienie obejmuje wsparcie oprogramowania przez okres 5 lat od dnia przyjęcia dostawy przez Zamawiającego. W ramach wsparcia oprogramowania Zamawiający zostanie uprawniony do pobierania zmian/ulepszeo, napraw/usprawnieo (update i upgrade), pobierania poprawek (krytycznych i opcjonalnych) i aktualizacji oprogramowania przez wskazany okres, w sposób nienaruszający praw twórców i właściciela praw autorskich oraz nieograniczający praw Zamawiającego do korzystania z oprogramowania. W przypadkach, kiedy w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”. Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki produkt, który posiada parametry techniczne i/lub funkcjonalne oraz spełnia wymagania co najmniej równe do określonych w OPZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego. Dla jednoznacznej identyfikacji oferowanego oprogramowania należy podać pełną nazwę produktu wraz z nazwą producenta. Zamawiający będzie weryfikował zgodność oferty z OPZ z informacjami producentów udostępnianymi na		

		stronach internetowych. Równoważne oprogramowanie musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: W zakresie dostawy oprogramowania równoważnego: 1. We wszystkich miejscach niniejszego dokumentu, w których użyto przykładowego znaku towarowego, patentu lub pochodzenia, jest to uzasadnione specyfiką przedmiotu zamówienia i Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń. 2. Wykonawca, który powoła się na oprogramowanie równoważne w zakresie opisanym przez Zamawiającego, jest obowiązany wykazać w ofercie, że oferowany przez niego przedmiot dostawy spełnia wymagania określone przez Zamawiającego. 3. Ciężar dowodowy w zakresie udowodnienia równoważności zaoferowanego oprogramowania z opisanymi warunkami równoważności spoczywa na Wykonawcy, składającym ofertę równoważną. 4. Zamawiający wymaga, aby zaoferowane przez Wykonawcę oprogramowanie równoważne nie powodowało konieczności wykonania dodatkowych prac integracyjnych po stronie Zamawiającego, tym samym poniesienia dodatkowych, niezaplanowanych kosztów. 5. W celu potwierdzenia, iż oferowana dostawa spełnia wymagania określone przez Zamawiającego, Wykonawca, który zaoferuje oprogramowanie równoważne do wskazanego przez Zamawiającego załączy do oferty szczegółową specyfikację techniczną dla oferowanego oprogramowania równoważnego, wystawioną przez producenta oferowanego oprogramowania równoważnego, zawierającą opis wszystkich cech i funkcjonalności oferowanego oprogramowania równoważnego. W przypadku dostarczenia równoważnego oprogramowania biurowego, o którym mowa w pkt 3 specyfikacji technicznej stanowiącej załącznik nr 3 do niniejszej umowy, Wykonawca zobowiązany jest przedłożyć Zamawiającemu harmonogram szkoleń organizowanych dla użytkowników równoważnego systemu operacyjnego. Szkolenia będą organizowane w siedzibie Zamawiającego. Harmonogram szkoleń musi zawierać: miejsce, terminy i godziny, w których będą odbywały się szkolenia oraz liczbę osób do przeszkolenia. Rozpoczęcie szkoleń warunkuje się zatwierdzeniem przez Zamawiającego harmonogramu szkoleń. Wykonawcę obowiązuje konieczność pisemnego zgłaszania Zamawiającemu każdorazowej zmiany harmonogramu z minimum dwudniowym wyprzedzeniem. Terminy szkoleń mogą ulec zmianie, wyłącznie na podstawie pisemnej zgody Zamawiającego. Potwierdzeniem wykonania szkoleń przez Wykonawcę będzie sporządzona przez Wykonawcę i podpisana przez każdego z użytkowników zestawu sprzętu komputerowego lista obecności wraz z potwierdzenie ilości godzin odbytego szkolenia.		
5.	Serwer kopii zapasowych	**Wskazanie urządzenia:** QNAP 4-Bay TS-431XeU-8G lub równoważny. **Typ**: Macierz dyskowa NAS. W ofercie wymagane jest podanie modelu, symbolu oraz nazwy producenta urządzenia. **Obudowa**: Obudowa typu Rack o wysokości minimalnie1U. Urządzenie dostarczone wraz z kompletem szyn umożliwiających montaż w szafie rack. Wymiary max.(wys. x szer. x gł.)44 × 439 × 291 mm **Procesor**:: Zainstalowany min. jeden procesor cztero- rdzeniowy dedykowany do pracy z zaoferowanym urządzeniem. Taktowanie bazowe 1.7GHz **Pamięć systemowa** - Min. 8 GB DDR3. **Możliwa pojemność pamięci** - Min. 8 GB **Pamięć flash** - Min. 512 MB.	1 szt	

		Dyski twarde - Zainstalowane 4 x min. 4TB, SATA/600, 256MB cache SATA 6 Gb/s. Technologia SMR Zgodność z systemami NAS Zaawansowane formatowanie (AF) Gwarancja 36 m-cy W ofercie wymagane jest podanie modelu, symbolu oraz nazwy producenta zaoferowanych dysków. **Kompatybilność dysków** 3,5-calowe dyski twarde SATA. 2,5-calowe dyski twarde SATA. 2,5-calowe dyski SSD SATA. **Obsługa modułów rozszerzających** - Tak **Możliwość wymiany dysków podczas pracy** - Tak. Port 10 Gigabit sieci Ethernet - Min. 1 x 10GbE SFP+ Port Gigabit sieci Ethernet - Min. 2x Gigabit RJ45 LAN. Gniazdo PCIe - Min.1 x PCIe 3.0 x4. Port USB - Min. 4 x USB 3.0 Panel użytkownika i oprogramowanie dostępne w języku polskim - Tak **Wymagania programowe** Kompatybilność z użytkowaną przezZamawiającego z platformą Q'center,pozwalającą na aktywne monitorowanie stanu serwerów NAS. **Zasilanie**: Otwarta rama 100 W, wejście: 100–240 V ~ / 3,5 A, 50–60 Hz **Obsługiwane poziomy RAID**: 0, 1, 10, 5, 6, JBOD; możliwość wyznaczenia dysku zapasowego **Zabezpieczenie danych**: 256-bitowe szyfrowanie AES na poziomie woluminów, szyfrowanie dysków zewnętrznych **Wbudowany serwer VPN oraz MySQL** – Tak Możliwość działania jako rejestrator do zbudowania wydajnego systemu monitoringu z kamerami IP – Tak **Obsługiwane systemy plików i funkcje dodatkowe** - EXT4, EXT3, NTFS, FAT32, HFS+, możliwość wykonania do 256 kopii migawkowych wolumenów, możliwość logicznego połączeni dysków o różnej prędkości (HDD i SSD) i włączenia automatycznego warstwowania danych tak aby najczęściej używane dane był automatycznie umieszczane na szybszych dyskach **Dostęp do danych z pracy oraz z dowolnego miejsca na świecie** – Tak **Serwer VPN (PPTP + OpenVPN + L2TP**) – TAK **Obsługiwane systemy operacyjne** - Mac OS 10.7 lub nowszy, Linux, UNIX, Windows 7/8, Windows 10, Microsoft Windows Server 2003,Microsoft Windows Server 2008, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019 **Obsługiwane protokoły i standardy** - TCP/IP - Transmission Control Protocol/Internet Protocol, DHCP Client - Dynamic Host Configuration Protocol Client, DHCP Server - Dynamic Host Configuration Protocol Server, CIFS/SMB, AFP 3.3,FTP - protokół transmisji plików, FTP/FTPS - protokół transmisji plików, http, HTTPS - Hypertext Transfer Protocol Secure, Telnet, SSH - Secure Shall, iSCSI - Internet SCSI, SNMP - Simple Network Management Protocol, SMTP, UPnP - Universal plug-and-play, RSYNC , WebDAV - Web Distributed Authoring and Versioning, LDAP (Lightweight Directory Access Protocol), DDNS - Dynamic Domain Name System, SSL - Secure Sockets Layer, TLS - Transport Layer Security, PPTP - Point to Point		

		Tunneling Protocol, AES - standard szyfrowania danych, FXP - File eXchange Protocol, OpenVPN client Zabezpieczenie Kensington lock – Tak Zarządzanie –SMNP Gwarancja producenta Min. 3 lata z możliwością przedłużenia do 5 lat		
6.	Serwer aplikacji	Obudowa • Typu Tower; • Możliwość dokupienia dedykowanego przez producenta serwera zestawu do montażu w szafie RACK; Płyta główna • Jednoprocesorowa; • Wyprodukowana i zaprojektowana przez producenta serwera • Możliwość instalacji procesorów 8-rdzeniowych; • Możliwość zainstalowania modułu TPM 2.0 • 4 złącza PCI Express generacji 3, w tym: o 2 fizyczne złącza o prędkości x8; o 1 fizyczne złącze o prędkości x4; o 1 fizyczne złącze o prędkości x1; o Możliwość zainstalowania risera umożliwiającego instalację kart „legacy PCI” • 4 gniazda pamięci RAM; • 4 zintegrowane porty SATA z możliwością konfiguracji RAID 0, 1, 10 oraz wsparciem dla systemów z rodziny Windows i Linux • Wsparcie dla technologii: o Dual Channel o ECC Procesory • Procesor 4-rdzeniowy • architektura x86 • Taktowanie 3,4GHz • 8MB pamięci cache Pamięć RAM • 16 GB pamięci RAM • DDR4 Registered • 2666Mhz • Możliwość zainstalowania 128GB pamięci RAM Dyski twarde i napędy • Minimum 4 wnęki dla dysków twardych Hotplug 3,5”; • Zainstalowany napęd DVD-RW	1 szt	

		• Zainstalowane 2 szt. HDD SATA 2TB HOT PLUG 3.5"; Kontrolery LAN • Trwale zintegrowana karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 1Gbit Base-T ze wsparciem iSCSI, WoL oraz PXE boot; Kontrolery I/O • Możliwość zainstalowania dwóch nośników flash o pojemności 64GB w konfiguracji RAID-1 rozwiązanie dedykowane dla hypervisora, rozwiązanie niezajmujące zatok dla dysków hot-plug Porty • Zintegrowana karta graficzna ze złączem VGA z tyłu serwera • 2 porty USB 3.0 na panelu przednim; • 4 porty USB 2.0 dostępne z tyłu serwera; • 2 porty USB 3.0 dostępne z tyłu serwera; • 1 port serial; • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera; Zasilanie, chłodzenie • Zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy nie większej niż 460W; • Redundantne wentylatory hotplug; Zarządzanie • Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera; • Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: o Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; o Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; o Dostęp poprzez przeglądarkę Web, SSH; o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; o Zarządzanie alarmami (zdarzenia poprzez SNMP) o Możliwość przejęcia konsoli tekstowej o Możliwość zarządzania przez 6 administratorów jednocześnie o Opcjonalne przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) o Obsługa serwerów proxy (autentykacja) o Obsługa VLAN o Możliwość konfiguracji parametru Max. Transmission Unit (MTU) o Wsparcie dla protokołu SSDP o Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3		

		○ Obsługa protokołu LDAP ○ Integracja z HP SIM ○ Synchronizacja czasu poprzez protokół NTP ○ Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); • Możliwość zainstalowania dedykowanej (lub zintegrowanej) pamięci flash o pojemności minimum 16 GB; Pamięć umożliwiająca możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN oraz umożliwiającej możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej. Opcjonalna możliwość zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; Wspierane OS • Microsoft Windows Server 2019, 2016 • VMWare vSphere 6.7, 6.5 • Suse Linux Enterprise Server 12 • Red Hat Enterprise Linux 7 Zainstalowany OS Zainstalowany system Microsoft Windows Serwer 2019 Essentials lub równoważny Gwarancja • 5 lat gwarancji producenta serwera w trybie onsite z gwarantowanym przyjazdem do miejsca użytkowania sprzętu certyfikowanego przez producenta pracownika serwisu do końca następnego dnia roboczego; • Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych; • Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; • Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty); Dokumentacja, inne		

		• Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymaganie oświadczenie wykonawcy lub producenta; • Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; • Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki; • W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; • Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; Możliwość wykonania aktualizacji BIOS z nośnika USB W przypadku dostarczenia równoważnego oprogramowania biurowego, o którym mowa w pkt 3 specyfikacji technicznej stanowiącej załącznik nr 3 do niniejszej umowy, Wykonawca zobowiązany jest przedłożyć Zamawiającemu harmonogram szkoleń organizowanych dla użytkowników równoważnego systemu operacyjnego. Szkolenia będą organizowane w siedzibie Zamawiającego. Harmonogram szkoleń musi zawierać: miejsce, terminy i godziny, w których będą odbywały się szkolenia oraz liczbę osób do przeszkolenia. Rozpoczęcie szkoleń warunkuje się zatwierdzeniem przez Zamawiającego harmonogramu szkoleń. Wykonawcę obowiązuje konieczność pisemnego zgłaszania Zamawiającemu każdorazowej zmiany harmonogramu z minimum dwudniowym wyprzedzeniem. Terminy szkoleń mogą ulec zmianie, wyłącznie na podstawie pisemnej zgody Zamawiającego. Potwierdzeniem wykonania szkoleń przez Wykonawcę będzie sporządzona przez Wykonawcę i podpisana przez każdego z użytkowników zestawu sprzętu komputerowego lista obecności wraz z potwierdzenie ilości godzin odbytego szkolenia.		
7.	**Switch zarządzany**	Łączna przepustowość - 70 Gb/s Przepustowość przełączania - 140 Gb/s Prędkość przekazywania pakietów - 104,16 Mp/s Maksymalny pobór mocy - 56 W Sposób zasilania - AC; 100 - 240 V AC / 50 - 60 Hz DC: 16 - 25 V, 56 W (wtyk DC 2,5 mm) Zasilacz - Wbudowany Diody LED na port Konsola: brak RJ45: Speed / Link / Activity SFP: Speed / Link / Activity Interfejsy sieciowe 48 gigabitowych portów Etrhernet 10/100/1000 Mb/s 2x SFP 2x SFP+ (1/10 Gb/s) Interfejs zarządzania 1x port RJ45 Ethernet In/Out Band		

		Wymiary - 443x43x286 mm Waga - 3,65 kg Możliwość montażu w szafie Rack Tak, wysokość 1U Certyfikaty CE, FCC, IC Ochrona ESD/EMP 24 kV Dopuszczalna temperatura pracy - Od -5 do 40 st. C Dopuszczalna wilgotność powietrza - 5%-95% niekondensująca Wstrząsy i wibracje - ETSI300-019-1.4 Główne funkcje przełączania: • ANSI/TIA-1057: LLDP-Media Endpoint Discovery (MED) • IEEE 802.1AB: Link Layer Discovery Protocol (LLDP) • IEEE 802.1D: Spanning Tree • IEEE 802.1S: Multiple Spanning Tree • IEEE 802.1W: Rapid Spanning Tree • IEEE 802.1Q: Vierual LAN with Port-Base VLANs • IEEE 802.1p: Ethernet Priority with User Provisioning and Mapping • IEEE 802.1X: port-based authentication with Guest VLAN support • IEEE 802.3: 10BASE-T • IEEE 802.3u: 100BASE-T • IEEE 802.3ab: 1000BASE-T • IEEE 802.1ak: Virtual Bridged Local Area Networks - Amendment 07: Multiple Registration Protocol • IEEE 802.3ac: VLAN Tagging • IEEE 802.3ad: Link Aggregation • IEEE 802.3x: Flow Control • IEEE 802.1D-2004: Generic Attribute Registration Protocol: Clause 12 (GARP) • IEEE 802.1D-2004: Dynamic L2 multicast registration: Clause 10 (GMRP) • IEEE 802.1Q-2003: Dynamic VLAN registration: Clause 11.2 (GVRP) • RFC4541: Considerations for Internet Group Management Protocol (IGMP) Snooping Switches • RFC 5171: Unidirectional link Detecion (UDLD) protocol Zaawansowane funkcje warstwy Layer 2 • Broadcast Storm Recovery • Broadcast / Multicast / Unknown Unicast Storm Recovery • DHCP Snooping • IGMP Snooping Querier • Independet VLAN Learning (IVL) • Jumbo Ethernet Frame Support • Port MAC Locking • Port Mirroring		

		• Protected Ports • Static MAC Filtering • TACACS+ • Voice VLAN • Unauthenticated VLAN • Internal 802.1X Authentication Server Pozostałe funkcje • DHCP Server: max 8 number of pools, max 128 number of leaser • Routing: 16 routes, 15 routing interfaces • VLANs: 155 • MAC Address: 8k • MSTP Instances: 4 • LAGs: 6 • ACLs: 100 with 10 rules per port • Traffic Classes (Queues): 8 Właściwości systemowe • Event and error logging facility • Run-Time and configuration download capability • PING utility • FTP/TFTP transfers via IPv4/IPv6 • Malicious Code Detection • BootP and DHCP • RFC 2021: Remote Network Monitoring Management Information Base Version 2 • RFC 2030: Simple Network Time Protocol (SNTP) • RFC 2819: Remote Network Monitoring Management Information Base • RFC 2865: RADIUS Client • RFC 2866: RADIUS Accounting • RFC 2868: RADIUS Attributes for Tunnel Protocol Support • RFC 2869: RADIUS Extensions • RFC 3579: RADIUS Support for EAP • RFC 3580: IEEE 802.1X RADIUS Usage Guidelines • RFC 3164: BSD Syslog Protocol Zarządzanie • Interfejs graficzny Web • CLI • Zarządzanie Ipv6		

		• Password Management • Autoinstall Support for Firmware Images and Configuration Files • SNMP v1, v2, v3 • SSH 1.5 / 2.0 • Secure Copy (SCP) • Telnet (Multi-Session Support) Layer 3 routing • Static Routing • Policy Based Routing Pozostałe parametry • Certyfikaty: CE, FCC, IC • Temperatura pracy: -5 do 40°C • Wilgotność podczas pracy: od 5 do 95% bez kondensacji • Wstrząsy i wibracje: ETSI300-019-1.4 Standard Informacje o gwarancji: Gwarancja 12 miesięcy liczona od daty sprzedaży		
8.	**Oprogramowanie antywirusowe**	**Obsługiwany System Operacyjny Windows:** **<u>Obsługiwane Systemy Operacyjne Komputerów</u>** Pełne wsparcie: Windows 11 (initial) Windows 10 November 2021 Update (21H2) Windows 10 May 2021 Update (21H1) Windows 10 October 2020 Update (20H2) Windows 10 May 2020 Update (20H1) Windows 10 November 2019 Update (19H2) Windows 10 May 2019 Update (19H1) Windows 10 October 2018 Update (Redstone 5) Windows 10 April 2018 Update (Redstone 4) Windows 10 Fall Creators Update (Redstone 3) Windows 10 Creators Update (Redstone 2) Windows 10 Anniversary Update (Redstone 1) Windows 10 November Update (Threshold 2)	**44 szt**	

		Windows 10 Windows 8.1 Windows 8 Windows 7 **<u>Windows Tablet oraz systemy wbudowane</u>** Pełne wsparcie Windows 10 IoT Enterprise Windows Embedded 8.1 Industry Windows Embedded 8 Standard Windows Embedded Standard 7 Windows Embedded Compact 7 Windows Embedded POSReady 7 Windows Embedded Enterprise 7 **<u>Systemy operacyjne serwera</u>** Pełne wsparcie Windows Server 2019 Core Windows Server 2019 Windows Server 2016 Windows Server 2016 Core Windows Server 2012 R2 Windows Server 2012 Windows Small Business Server (SBS) 2011 Windows Server 2008 R2 **<u>Systemy Operacyjne Linux</u>** Ubuntu 14.04 LTS lub wyższy Red Hat Enterprise Linux / CentOS 6.0 lub wyżej SUSE Linux Enterprise Server 11 SP4 lub wyższy OpenSUSE Leap 42.x Fedora 25 lub wyższy Debian 8.0 lub wyższy Oracle Linux 6.3 lub nowszy Amazon Linux 2		

		Amazon Linux AMI 2016.09 lub nowszy **<u>Systemy Operacyjne Mac OS X</u>** • macOS Big Sur(11.0) • macOS Catalina (10.15) • macOS Mojave (10.14) • macOS High Sierra (10.13) • macOS Sierra (10.12) • OS X El Capitan (10.11) **Wymagania Ochrony Mobile[3]** ● Apple iPhone i tablety iPad (iOS 8.1+) ● Smartfony i tablety z Google Android (4.2+) **Obsługiwane Środowiska Microsoft Exchange** Security for Exchange wspiera następujące wersje i role Microsoft Exchange: • Exchange Server 2019 z rolą Edge Transport lub Mailbox • Exchange Server 2016 z rolą Edge Transport lub Mailbox • Exchange Server 2013 z rolą Edge Transport lub Mailbox • Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox • Exchange Server 2007 z rolą Edge Transport, Hub Transport lub Mailbox Security for Exchange jest kompatybilny z Microsoft Exchange Database Availability Groups (DAG). **Ochrona środowisk wirtualnych (SVE)** 1. Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej 2. Maszyna wirtualna pełniąca rolę silnika skanującego może być pobrana w formacie: a) OVA b) XVA c) VHD d) VMDK Środowiska wspierane: ● VMware vSphere & vCenter Server 7.0 update 1, 7.0, 6.7 update 3, update 2a,6.7 update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0 ● VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x ● VMware Workstation 11.x, 10.x, 9.x, 8.0.6 ● VMware Player 7.x, 6.x, 5.x ● Citrix XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (including Xen Hypervisor) ● Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906		

		● Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR ● Citrix VDI-in-a-Box 5.x ● Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 20 (including Hyper-V Hypervisor) ● Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor) ● Oracle VM 3.0 ● Oracle VM VirtualBox 5.2, 5.1 ● Nutanix Prism with AOS 5.5, 5.10, 5.15 LTS ● Nutanix Prism with AOS 5.6, 5.11, 5.18 STS ● Nutanix Prism with AHV 20170830. **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[3] 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 wykluczeni 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 umożliwia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS. 21. Program skanuje 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 będzie pytał o hasło. 23. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie" możliwość zdefiniowania przez administratora 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. Obsługa 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 wbudowana funkcje 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, lekkiego ze sprawdzaniem reputacji plików w chmurze, lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego. 42. Maszyna która przejmuję rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji 43. Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego. 44. Możliwość tworzenia list sieci zaufanych. 45. Możliwość dezaktywacji funkcji zapory sieciowej. 46. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. 47. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware 48. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji 49. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań(konfigurowalne w politykach bezpieczeństwa) 50. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups 51. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego. 52. System zarządzania ryzykiem[2] – 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 niezwyczajnych 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 53. 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) <u>Uwaga: Ta warstwa zabezpieczeń dotyczy systemów opartych na systemie Windows.</u> 54. Ochrona poczty(add-on[1,2]) – mechanizm pozwalający na ochronę poczty Office 365 lub Microsoft Exchange z wykorzystaniem serwera pośredniczącego. 55. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak: -Wczesny dostęp -Dostęp do poświadczeń -Wykrycie -Crimeware		

		56. Pełne Szyfrowanie dysków(add-on[1]) 57. Zarządzanie aktualizacjami oprogramowania firm trzecich(add-on[1]) 58. 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|xlsm|xlsx|xml| Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania. 59. Ochrona proaktywna oparta o maszynowe uczenie która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak: a) Ukierunkowane ataki b) Podejrzane pliki i ruch w sieci c) Exploity d) Ransomware e) Grayware 60. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego 61. Moduł ochrony proaktywnej musi działać w trybach które administrator może dowolnie zmieniać na: a) Tolerancyjny b) Normalny c) Agresywny 62. Zintegrowany sandbox po stronie producenta który pozwala na analizę pliku a) Plik może zostać wysłany automatycznie ze stacji roboczej jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora b) Możliwość przesłania archiwum zabezpieczonego hasłem		

		c) Możliwość przesłania adresu URL d) W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo. 63. Wbudowany sandbox musi działać w trybie monitorowania i blokowania 64. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny 65. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania. 66. Wbudowany sandbox musi posiadać opcję która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa. 67. Minimalny rozmiar pliku jaki może zostać przesłany do sandboxa to 1KB 68. Maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa to 50MB 69. Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń oraz daje możliwość: a) Filtrowania zdarzeń b) Blokowania procesów c) Dodawanie procesów do czarnej listy d) Dodawanie procesów do białej listy e) Izolacja hosta f) Aktualizacja oprogramowania firm trzecich na hoście(1) g) Przesłanie pliku do Sandbox h) Sprawdzenie informacji o pliku w Google i) Sprawdzenie informacji o pliku w VirusTotal 70. Filtrowanie zdarzeń odbywa się na podstawie: a) Ocena zagrożenia od 10 do 100 punktów b) Data wykrycia c) Status d) ID		

		e) Nazwa punktu końcowego f) Typ ataku a) Ransomware b) Potencjalnie niechciana aplikacja c) Malware d) Exploit e) Fileless f) Password stealer g) Downloader h) Inne i) Zdefiniowane przez użytkownika 71. Wyszukiwanie zdarzeń może odbywać się na podstawie: a) Nazwa alertu b) IP punktu końcowego c) Hash MD5 d) Hash SHA256 e) Nazwa użytkownika 72. Możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń które mają najczęściej problem. 73. Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie. 74. Możliwość wyświetlenia zablokowanych hashy plików. 75. Możliwość dodania własnych hashy MD5 oraz SHA256 76. Możliwość importu hashy z pliku CSV 77. Możliwość filtrowania dodanych hashy na podstawie: a) Typu hashu		

		b) Wartości hash c) Źródło dodania d) Informacje o źródle e) Nazwa pliku f) Firma której dotyczy wpis[2] g) Możliwość wyświetlenia 10,20,30,50,100 wpisów na jednej stronie. **Hypervisor Introspection HVI - Wgląd w pamięć hypervisora (add-on[1,3])** ***Wymagania minimalne:*** 1. Architektura CPU: – dowolny Intel® Sandy Bridge bądź późniejszy, wspierający Intel® Virtualization Technology. – rozszerzenia VT-x or VT-d muszą być włączone w BIOS 2. Citrix XenServer 7 Enterprise Edition bądź wyższy 3. Komputery muszą działać na wspieranym systemie operacyjnym: 1. Systemy operacyjne Windows dla komputerów Desktop – Windows 10 – Windows 8.1 – Windows 8 – Windows 7 2. Systemy operacyjne Windows Server – Windows Server 2016 – Windows Server 2012 / Windows Server 2012 R2 – Windows Server 2008 R2 3. Systemy operacyjne Linux – Debian 9, 64-bit – Debian 8, 64-bit – Ubuntu 16.04 LTS, 64-bit – Ubuntu 14.04 LTS, 64-bit – CentOS 7, 64-bit – Red Hat Enterprise Linux 7, 64-bit – SUSE Linux Enterprise Server 12, 64-bit – Oracle Linux 7.3, 64-bit ***Cechy:*** 1. Rozwiązanie integruje się z technologią hypervisor aby zapewnić nie wymagającą agenta ochronę dla goszczących maszyn wirtualnych (nie jest konieczna instalacja agenta ani/i sterownika na maszynie wirtualnej gościa). 2. Rozwiązanie chroni pamięć, zarówno w systemie operacyjnym Windows jak i Linux. 3. Rozwiązanie monitoruje system operacyjny w trybie użytkownika i trybie pamięci kernela. 4. Rozwiązanie monitoruje i chroni następujące komponenty przestrzeni jądra:		

		1. Rejestry kontrolne. 2. Rejestry specyficzne dla modelu. 3. Spójność IDT/GDT. 4. Załadowane sterowniki. 5. Rozwiązanie oferuje dodatkowe szczegóły technik śledczych, raportowane do konsoli zarządzającej: 1. Awarie systemu operacyjnego. 2. Zdarzenia związane ze sterownikami. 3. Zdarzenia związane z awarią aplikacji. 6. Rozwiązanie oferuje mechanizmy wglądu hypervisora w celu uzyskania dostępu do czystej pamięci maszyny wirtualnej i wykrywa jej naruszenia wywołane technikami ataku takimi jak heap spray, przepełnienie bufora czy iniekcja kodu. 7. Rozwiązanie oferuje alerty, powiadomienia i raportowanie zdarzeń osiągalne w scentralizowanej konsoli zarządzania. 8. Bazując na wykrywaniu naruszeń pamięci, rozwiązanie jest w stanie wprowadzić narzędzie naprawcze do działającej maszyny wirtualnej aby zgromadzić dodatkowe szczegóły do analizy śledczej i wykonać pełny skan antymalware systemu; narzędzie naprawcze ma zdolność usunięcia się kiedy naprawa zostanie wykonana. 9. Rozwiązanie pozwala administratorom IT lub grupom zajmującym się bezpieczeństwem na wprowadzenie zewnętrznych narzędzi do maszyn wirtualnych bez żadnej interakcji z użytkownikiem bądź połączeniem sieciowym. 10. Narzędzia zewnętrzne muszą mieć opcje bycia wprowadzonymi manualnie, automatycznie bądź też według harmonogramu. **Urządzenia Mobilne[3]** 1. Dla systemu Android możliwość funkcja blokowania stron internetowych 2. Możliwość szyfrowania urządzenia opartego o system android. 3. Możliwość pobrania wersji instalacyjnej ze sklepu iOS oraz Android 4. Skanowanie aplikacji w trakcie instalacji na urządzeniach z systemem Android 5. Posiadać możliwość wymuszenia szyfrowania urządzenia dla systemu Android 6. Możliwość blokowania ekranu głównego hasłem.		

		7. Możliwość definiowania połączeń WiFi 8. Kontrola przeglądarki Safari dla urządzeń z systemem iOS **Maszyny Wirtualne** **1.**Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu) **2.**Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej. **3.**Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem **4.**Wersja kliencka nie pełni roli ochrony antywirusowej, jest tylko agentem dla Security Servera. **5.** Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym. **6.** Możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta. **7.** Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny. **8.** Możliwość wskazania do jakiego serwera ochrony maja się łączyć klienci maszyn wirtualnych. **Stacje robocze i serwery Windows** **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 oraz sygnatury muszą być aktualizowane nie rzadziej niż raz na godzinę. **10.** Oprogramowanie musi posiadać możliwość raportowania zdarzeń informacyjnych. **11.** Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju. **12.** Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych 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 wykorzystania dodatkowej maszyny wirtualnej która przejmie role silnika skanującego. **17.** Możliwość określenia jak długo maja 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. **Ochrona Exchange** 1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego. 2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w przeciągu ostatnich kilku godzin / dni. 3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz nie możliwych do przeskanowania. 4. Możliwość wykluczenia potencjalnie niechcianych aplikacji (PUA) z filtrowania antymalware. 5. Możliwość skanowania w poszukiwania malware wewnątrz archiwów. 6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen. 7. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera. 8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy. 9. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi. 10. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowania maila do konkretnej skrzynki pocztowej.		

		11. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością. 12. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki. **Konsola zdalnej administracji** 1. Dwa typy konsoli administracyjnej: • Konsola Cloud – serwer administracyjny po stronie producenta • Konsola On-premise – lokalny serwer administracyjny 2. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows. 3. 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. 4. Możliwość integracji Domeny Active Directory w obu typach konsoli. 5. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych. 6. 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). 7. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi 8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego. 9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu. 10. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej. 11. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa. 12. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej. 13. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv 14. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.		

		15. Możliwość generowania raportu co godzinę. 16. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu. 17. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej. 18. Możliwość dodania etykiety do stacji roboczej. 19. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej. 20. Możliwość przechowywania kwarantanny maksymalnie 180 dni 21. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać. 22. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny. 23. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej. 24. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym.[3] 25. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania. 26. 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. 27. 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 28. Integracja z serwerem Syslog[3] 29. Uwierzytelnienie dwuskładnikowe realizowane wyłącznie przez aplikację Google Authenticator		

		30. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni[2] 31. Możliwość zablokowania konta w konsoli jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem[2] 32. Funkcja pojedynczego logowania – Single Sign-on (SSO)[2] 33. Możliwość naprawy instalacji z poziomu konsoli[2] 34. Raport streszczający[2] - 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 35. 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[2] 36. 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 okrślenie godziny kiedy te maszyny będą usuwane 37. Możliwość określenia własnego serwera NTP[3] 38. Integracja z vCenter Server[3] 39. Integracja z Xen Server[3] 40. Integracja z nutanix Prism Element[3] 41. Możliwość integracji z Amazon EC2 42. Intergracja z Azure[3] 43. Każdy z rodzajów ochrony musi być rozdzielony w osobnych oknach konfiguracyjnych, komputery fizyczne, Urządzenia mobilne. 44. Serwer centralnej administracji musi posiadać funkcje przełączenia się miedzy widokiem maszyn fizycznych i urządzeń mobilnych. Tak by wyświetlana była jedynie wskazana grupa urządzeń chronionych. 45. Tworzenie osobnych polityk dla fizycznych komputerów, urządzeń mobilnych oraz maszyn wirtualnych. 46. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony. 47. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego. 48. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej. 49. Pion firmy[2] - 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 50. Funkcja kontroli aplikacji która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów. (3) 51. Funkcja kontroli aplikacji może działać w trybie testowym lub produkcyjnym 52. Funkcja kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat. (3) 53. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta. 54. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS 56. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym. 57. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni. 58. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS 59. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1 60. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych(2). 61. Możliwość skanowania SSL dla połączeń RDP(2)		

		62. Oprogramowanie umożliwia ochronę kontenerów instalowaną bezpośrednio na hoście kontenera oferuje wgląd w złośliwą aktywność serwera Linux i kontenerów w czasie rzeczywistym. Przypisy **[1]Add-on jest modułem opcjonalnym, dodatkowo płatnym który należy zakupić oddzielnie** **[2] Usługa dostępna tylko w wersji cloud.** **[3] Usługa dostępna tylko w wersji on-premise**		
8	Firewall UTM	**1.1.1 System zabezpieczenia sieci wewnętrznej LAN oraz dostępu do Internetu przy użyciu full-state Inspection Firewall nowej generacji.** Należy dostarczyć i wdrożyć urządzenie typu Zapora Sieciowa Nowej Generacji (NGFW) która wymuszać będzie przyjętą/wdrożoną politykę bezpieczeństwa. NGFW musi posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall'a, systemu ochrony IPS oraz usług sieciowych takich jak np. DHCP Server; VPN Gateway; Application Control. Oferowany w ramach postępowania sprzęt musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego producenta w Polsce. Klaster zapór sieciowych musi spełniać następujące kryteria: 1.1.1.1 Zapora sieciowa (Firewall) a) Urządzenie musi umożliwiać inspekcję stanową (full-state Inspection) opartą na granularnej analizie komunikacji sieciowej oraz rozpoznawaniu i analizie warstwy aplikacji w celu poprawnego śledzenia i kontroli przepływu ruchu. b) Urządzenie ma obsługiwać translacje adresów NAT typu: n:1, NAT1:1; PAT; Network MAP/NAT. c) Urządzenie musi posiadać możliwość ustawienia trybu pracy jako router/brama warstwy trzeciej, jako bridge warstwy drugiej (Transparent mode) oraz w trybie analizatora ruch TAP monitor port. d) Graficzny Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Administrator ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, serwisy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. e) Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i	**1**	

		wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola Quality Of Service, godziny oraz dnia obwiązywania (aktywnośic) reguły. f) Administrator ma możliwość zdefiniowania minimum sześciu (niezależnie konfigurowalnych) typów reguł/polityk na firewall'u. g) Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, pozwalający na sprawdzanie jaka reguła będzie stosowana dla danego typu ruchu i eliminujący sprzeczności w konfiguracji reguł h) Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, zewnętrzny serwer LDAP; Microsoft Active Directory z możliwością wdrożenia strategii autoryzacji wieloskładnikowej (Multi-Factor-Authentication MFA) 1.1.1.2 **<u>Intrusion Prevention System (IPS)</u>** a) Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. b) Moduł IPS musi posiadać bazę „na urządzeniu" co najmniej 10 000 sygnatur które są utrzymane i aktualizowane przez producenta. c) Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. d) Moduł IPS powinien wykrywać oraz blokować szkodliwą zawartość w kodzie HTML oraz Javascript. e) Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POPS oraz SMTPS. f) Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. g) Moduł skanujący musi działać na urządzeniu (firewall'u). Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci. h) Urządzenie w ramach działania modułu IPS musi posiadać możliwość powiadamiania o wykrytych podatnościach w ruchu wraz z informacją o kodzie CVE. i) Administrator musi mieć możliwość konfiguracji jednego z trybów pracy modułu proaktywnej ochrony i inspekcji pakietów IPS w zakresie: tryb aktywny IPS, tryb passywny IDS; musi być możliwość konfiguracji baza wyjątków modułu IPS dla wybranych adresów IP (źródłowych i docelowych), portów docelowych; sygnatur bazy CVE. 1.1.1.3 **<u>Kształtowanie pasma (Traffic Shapping)</u>**		

		a) Urządzenie musi pozwalać na kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. b) Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia z uwzględnieniem kierunku przesyłanych danych (upload / download). Kwalfikacja Traffic Shapping z uwzględnienim adresu IP (źródłowego i docelowego), portów docelowych; autoryzowanego użytkownika c) Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). d) Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. e) Traffic Shapping powinien działać w oparciu o profile QoS Band tzw. klasyfikatory ruchu które będą kolejkowane do fizycznych lub logicznych interfejsów firewall'a 1.1.1.4 <u>Ochrona antywirusowa</u> a) Rozwiązanie ma umożliwiać inspekcję przez skaner antywirusowy, co najmniej jeden silnik antywirusowy powinien być dostarczony przez firmę inną niż producent rozwiązania b) Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. c) Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji. Proponowany system powinien umożliwiać wysyłanie powiadomienia email o załączniku, który został zablokowany. d) Ochrona antyspam ma działać w oparciu o DNS RBL e) W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. 1.1.1.5 **<u>Wirtualne sieci prywatne (VPN)</u>** a) Urządzenie musi posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). b) Odpowiednio kanały VPN można budować w oparciu o: - PPTP VPN, - L2TP VPN - IPSec VPN,		

		- SSL VPN c) SSL VPN musi działać w trybach Tunel i Portal. d) W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. e) Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). f) Urządzenie ma posiadać wsparcie dla technologii XAuth oraz Hub 'n' Spoke. g) Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. h) Urządzenie musi być dostarczone wraz z dedykowanym klientem IPSec VPN. i) Rozwiązanie ma obsługiwać multitransport VPN – tworzenie do 24 transportów w obrębie jednego tunelu VPN site-to-site pomiędzy tymi samymi lokalizacjami, korzystających z różnych łączy i ustawień. j) Rozwiązanie ma zapewnić możliwość łączenia transportów VPN (agregacja łączy na poziomie pakietów, lub sesji) i wyznaczania transportów zapasowych. k) Rozwiązanie ma zapewniać kompresję i deduplikację danych przesyłanych w tunelach VPN. l) Rozwiązanie ma mieć możliwość buforowania danych przesyłanych w tunelach VPN dla protokołów zdefiniowanych przez administratora. 1.1.1.6 **<u>Filtr dostępu do stron WWW (URL filtering)</u>** a) Urządzenie musi posiadać wbudowany filtr URL. b) Filtr URL ma działać w oparciu o klasyfikację URL zawierającą kategorie tematyczne stron internetowych; wymagana ilość rozpoznawanych kategorii 86. c) Urządzenie powinno wspierać mechanizmy białych i czarnych list d) Urządzenie nie może posiadać ograniczenia w postaci limitu ilości białych i czarnych list definiowanych przez administratora e) Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. f) Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: - ·blokowanie dostępu do adresu URL, - ·zezwolenie na dostęp do adresu URL,		

		- ·blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. g) Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. h) Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. i) Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. j) Urządzenie musi dawać możliwość utworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. Baza wyjątków tworzona co najmniej przy użyciu dwóch metod: a. wskazanie/wpisanie docelowej domeny (np. *.skype.com; *.microsoft.com) ; b. wskazanie kategorii ruch (np. Bankowość i Finanse) k) Urządzenie musi umożliwiać włączenia pamięci cache dla ruchu http. l) Urządzenie musi wbudowany i rekonfigurowany WEB portal powiadomień zwrotnych służący do informowania użytkowników o nałożonych restrykcjach/ograniczeniach wynikających z wdrożonej polityki bezpieczeństwa (np. zablokowanie strony WWW danego portalu z powodu niedozwolonej kategorii) 1.1.1.7 **<u>Uwierzytelnianie</u>** a) Urządzenie musi zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: - lokalną bazę użytkowników, - zewnętrzną bazę użytkowników (zewnętrzny LDAP), - usługę katalogową Active Directory. b) Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. c) Rozwiązanie musi zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: - SSL, - Radius, - Kerberos. d) Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. e) Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny. 1.1.1.8 **<u>Administracja łączami do Internetu (ISP)</u>** a) Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). b) Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa		

		mechanizmy: - równoważenie względem adresu źródłowego, - równoważenie względem połączenia. c) Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. d) Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. e) Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. f) Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. g) Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. h) Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. i) Rozwiązanie powinno wspierać technologię Link Aggregation. 1.1.1.9 **<u>Pozostałe usługi i funkcje rozwiązania</u>** a) Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. b) Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. c) Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. d) Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci z możliwością określenia różnych bram, a także serwerów DNS e) Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. f) Urządzenie musi posiadać usługę DNS Proxy. 1.1.1.10 **<u>Administracja urządzeniem</u>** a) Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia. b) Konfiguracja urządzenia ma być możliwa z wykorzystaniem interfejsu graficznego w zakresie konfiguracji podstawowej i zaawansowanej. c) Urządzenie posiada możliwość eksportu informacji przez syslog. Wysyłanie logów powinno być możliwe do wielu serwerów, równocześnie.		

		d) Urządzenie wspiera eksport zdarzeń opartych o przepływy za pomocą protokołu NetFlow lub analogiczny np. protokołu IPFIX e) Komunikacja z interfejsem zarządzania może odbywać się na porcie innym niż https (443 TCP). f) Urządzenie powinno umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. g) Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. h) Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową lub poprzez dedykowaną aplikację do zarządzania a komunikacja musi być zabezpieczona (autoryzacja i szyfrowanie ruchu). i) Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. j) Urządzenie musi pozwalać na odtworzenie backupu konfiguracji w sposób: - bezpośrednio z centralnej konsoli zarządzania; - przywrócenie konfiguracji z lokalnego graficznego interfejsu zarządzania GUI - przywrócenie konfiguracji z lokalnego tekstowego interfejsu zarządzania (console port) - przywrócenie konfiguracji ze zdalnego trybu tekstowego zarządzania (SSH) - przywrócenie systemu operacyjnego i konfiguracji z użyciem klucza USB-Stick k) Zapory sieciowe muszą być wyposażone w aplikację lub system umożliwiający zdalne zarządzanie firewallem, serwerem VPN oraz pozostałymi serwisami z jednej graficznej konsoli administracyjnej pracującej przynajmniej pod kontrolą systemu Windows lub Linux. 1.1.1.11 **<u>Raportowanie</u>** a) Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. b) W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów. c) System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. d) Firewall musi posiadać ujednolicony pulpit (Dashboard) monitorujący i raportujący o bezpieczeństwie		

		chronionego środowiska IT z uwzględnieniem raportowania w przedziałach czasu (aktualna sytuacja do 60min; ostatnia godzina; ostatnie 24h; ostatni dzień; ostatnie 7dni; ostatni tydzień; obecny miesiąc; ostatni miesiąc) e) System raportujący powinien posiadać wbudowane wzorce gotowych raportów dotyczących min. aplikacji, aktywność użytkownika, użycia VPN, bezpieczeństwa sieci i oceny ryzyka. 1.1.1.12 **Parametry** a) Urządzenie musi posiadać dysk SSD o pojemności nie mniejszej niż 100 GB. b) Urządzenie w formie (hardware appliance) urządzenia sprzętowego posiadającego: - przynajmniej 5 portów 1000Base-T RJ45, - przynajmniej 1 port Console (RS232), - przynajmniej 2 porty USB. c) Wysokość urządzenia nie może przekroczyć 1U. e) Przepustowość firewalla: min. 2.0 Gb/s. f) Wydajność firewalla (włączona kontrola IPS): min. 600 Mb/s. g) Wydajność z włączonymi modułami ochrony IPS, Application Control, URL Filtering i Anti-Virus: min. 1.2Gbps w warunkach produkcyjnych (pakiety i sesje charakterystyczne dla ruchu do Internetu). h) Przepustowość tunelu VPN przy szyfrowaniu AES-128: min. 720 Mb/s. i) Obsługa sieci logicznych min. 256 VLAN j) Liczba równoczesnych sesji - min. 80 000 i nie mniej niż 12 000 nowych sesji/sekundę. k) Rozwiązanie musi mieć możliwość rozbudowy do działania w układzie klastra niezwodnościowego HA w trybie Active/Pasive. l) Urządzenie powinno wspierać tworzenie tuneli VPN za pomocą graficznego interfejsu w modelu Drag&Drop bez potrzeby użycia narzędzi konsolowych (command line). m) Urządzenie musi zapewniać możliwość integracji z platformą zarządzania wszystkimi urządzeniami, pracującymi w strukturze geograficznie rozproszonej w wielu lokalizacjach jednocześnie (Zamawiający planuje w przyszłości zakup dodatkowych urządzeń). n) Urządzenie musi posiadać dedykowany port konsoli ze złączem RS232 lub RJ45 o) Wyposażenie w elementy umożliwiające montaż urządzenia w 19" szafie stelażowej. p) Dostarczenie kompletu kabli kat 7A oraz OM4, wszystkich wkładek SFP, które mogą pochodzić od producenta innego niż producent zaaferowanych urządzeń. Wkładki SFP muszą być w pełni kompatybilne z zaoferowanymi		

		urządzeniami oraz posiadać co najmniej roczną gwarancję producenta. q) Uruchomienie zestawu w tym szczególnie instalacja i pełna konfiguracja firewalli według ustaleń projektowych zaakceptowanych przez Zamawiającego. Wymagany jest podstawowy i zaawansowany zakres konfiguracji. r) Poszczególne użyte do budowy zestawu komponenty sprzętowe nie mogą w żaden sposób ograniczać maksymalnej przepustowości i prędkości pracy zestawu. s) Zaoferowane urządzenia nie mogą być przewidziane przez producenta do zastąpienia nowszym modelem przez co najmniej trzy lata począwszy od dnia podpisania umowy. 1.1.1.13 **Licencje** Wszystkie dostarczone licencje w ramach rozwiązania muszą obejmować wymagany okres *36-miesięcy* i nie mogą posiadać limitu użytkowników. Wraz z urządzeniem wykonawca dostarczy wymagane do prawidłowej pracy licencje: - *36-miesięczna* subskrypcją na aktualizację: systemu operacyjnego; aktualizację sygnatur dla silnika IPS, aktualizację sygnatur dla silnika dynamicznego rozpoznawania aplikacji. - *36-miesięczna* subskrypcją na ochronę antywirusową; aktualizacje sygnatur spamu oraz dostęp do serwerów RBL DNS. - *36-miesięczna* subskrypcją na poszerzoną ochronę ATP (Sanboxing) w zakresie zawansowanej analizy załączników i ochrona przed zagrożeniami dnia zerowego; ochrona przed atakami typu ransomware. Wymagane aby analiza/ocena (wykonywana przez NGFW/ATP Services) bezpieczeństwa dla załącznika mailowego lub pobieranego pliku, była wykonywana w trybie bezpiecznym tzn. kwalifikacja zakresie poprawności/zdrowia załącznika lub pliku przed dostarczeniem do użytkownika. - System powinien mieć możliwość aktywacji funkcjonalności dostępu zdalnego w technologii dostęp zdalny w technologii SSL-VPN; urządzenie musi obsługiwać portal Usługowy w trybie HTTPS oraz umożliwiać zdalny dostęp (SSL-VPN) przy użyciu zunifikowanej aplikacji mobilnej; wymagana obsługa dwu-etapowej MFA / wieloskładnikowej metody autoryzacji. - *36-miesięczna* subskrypcja dostępu do platformy zarządzania umożliwiająca m.in.: o zapisywanie całej historii zmian konfiguracji urządzenia (administrator musi mieć możliwość powrotu do konfiguracji danego modułu z danego dnia oraz informację, jaki użytkownik wprowadził zmianę). Ponadto funkcja musi pozwalać na tworzenie audytów, które pokazują wszystkie zmiany dokonane w konfiguracji		

		wraz z informacją jaki użytkownik je wprowadził. o administrację urządzeniem opartą na rolach i współdzieleniu pracy kilku administratorów jednocześnie – system umożliwia jednoczesną pracę kilku administratorom i zapobiega konfliktom między administratorami oraz loguje wszystkie zmiany. o konfigurację urządzenia z wykorzystaniem aplikacji mobilnej do monitoringu; aplikacja musi być dostępna na co najmniej jednym z trzech systemów mobilnych (Windows Mobile/Android/iOS). Aplikacja musi umożliwiać co najmniej: prezentację ogólnych danych urządzenia (m.in. czas pracy, status licencji, wersja firmware, model i numer seryjny), wyświetlanie statusu urządzenia (obciążenie procesora i sieci, zużycia pamięci RAM oraz wykorzystania powierzchni dyskowej a także dane z czujników sprzętowych), dynamiczne prezentowanie wykresów dla: przepustowości, ilości sesji dozwolonych i zablokowanych, wykonanie restartu urządzenia, restartu usług, używanie pełnego dostępu terminalowego (SSH), włączanie i wyłączanie dynamicznych reguł zapory (na przykład w celu zapewnienia zespołowi tymczasowego dostępu do zablokowanych aplikacji internetowych). 1.1.1.14 **Gwarancja i wsparcie techniczne producenta** Minimum *36-miesięczna* gwarancja sprzętowa producenta obejmująca wszystkie elementy urządzenia zapewniająca w przypadku awarii wysłanie sprawnego sprzętu na wymianę urządzenia wg procedur RMA Producenta. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania oraz wsparcia technicznego producenta z czasem reakcji nie dłuższym niż 2 godziny od momentu zgłoszenia problemu. Wymagana jest dostępność usługi w trybie 8x5 w godzinach od 8:00 do 17:00 (e-mail; telefon; web-portal) Po upływie co najwyżej 4 lat Zamawiający musi posiadać możliwość nieodpłatnej wymiany sprzętu na fabrycznie nowe urządzenie w nowszej wersji sprzętowej w ramach tej samej serii/linii produktowej. 1.1.1.15 **Dodatkowe wymagania wdrożeniowo-instalacyjne** Wykonawca zobowiązuje się do wykonania uruchomienia zestawu(ów) kierując się zasadą utrzymania ciągłości dotychczas dostępnych usług u Zamawiającego. Dopuszcza się możliwość odejścia od tej zasady z zastrzeżeniem każdorazowego uzgadniania z Zamawiającym. 1.1.1.16 **Szkolenia** Wykonawca dostarczy Zamawiającemu vouchery na autoryzowane szkolenie Barracuda dla min. *X-osób.* Program szkolenia ma obejmować konfigurację urządzeń oraz właściwe użycie funkcji bezpieczeństwa. Szkolenie powinno zawierać przykłady rozwiązywanie typowych problemów związanych z zarządzaniem i diagnostyką dostarczonego rozwiązania.		

		Uczestnik szkolenia ma prawo (do nieopłatnego) przystąpienia do egzaminu końcowego w celu uzyskania oficjalnego certyfikatu producenta sprzętu. Czas szkolenie ma być nie mniejszy niż 3dni. Ważność voucherów ma być nie krótsza aniżeli 6 miesięcy. 1.1.1.17 <u>Wdrożenie</u> Opis zakresu wdrożenia jeśli jest wymagane.		
9	Pakiet oprogramowania biurowego	Pakiet oprogramowania biurowego w polskiej wersji językowej. Minimalna zawartość: 1)edytor tekstu 2) arkusz kalkulacyjny 3) program do tworzenia prezentacji 4) program do obsługi poczty e-mail - kalendarza 5) program do zbierania notatek Kompatybilny z Microsoft Office: **1)** otwieranie dokumentów utworzonych przy pomocy programów: MS Word 2019, MS Excel 2019, MS Power Point 2019, MS Word 2016, MS Excel 2016, MS Power Point 2016, MS Word 2013, MS Excel 2013, MS Power Point 2013, MS Word 2010, MS Excel 2010, MS Power Point 2010, MS Word 2007, MS Excel 2007, MS Power Point 2007, MS Word 2003, MS Excel 2003, MS Power Point 2003. W otwieranych dokumentach musi być zachowane oryginalne formatowanie oraz ich treść bez utraty jakichkolwiek ich parametrów i cech użytkowych (korespondencja seryjna, arkusze kalkulacyjne zawierające makra i formularze itp.) czy też konieczności dodatkowej edycji ze strony użytkownika, **2)** dostarczony pakiet musi zapewniać możliwość modyfikacji plików utworzonych za pomocą ww. programów w taki sposób by możliwe było ich poprawne otworzenie przy pomocy programu, który oryginalnie służył do utworzenia pliku, **3)** w przypadku programu do obsługi poczty e-mail możliwość bezproblemowego zaimportowania /wyeksportowania wszystkich danych (wiadomości e-mail, wpisy kalendarza, zadania, kontakty, reguły wiadomości) z i do używanych przez Zamawiającego programów Outlook 2003, Outlook 2007, Outlook 2010, Outlook 2013, Outlook 2016, Outlook 2019. Licencja na dostarczone oprogramowanie musi umożliwiać użytkowanie bezterminowe (dożywotnie), bez dostępu przez Internet, przy jednorazowej zapłacie za licencję. W przypadku dostarczenia równoważnego oprogramowania biurowego, o którym mowa w specyfikacji technicznej stanowiącej załącznik nr 1 do niniejszej umowy, Wykonawca zobowiązany jest przedłożyć	**11 szt**	

<table>
<tr><td></td><td></td><td>Zamawiającemu harmonogram szkoleń organizowanych dla użytkowników równoważnego systemu operacyjnego. Szkolenia będą organizowane w siedzibie Zamawiającego. Harmonogram szkoleń musi zawierać: miejsce, terminy i godziny, w których będą odbywały się szkolenia oraz liczbę osób do przeszkolenia. Rozpoczęcie szkoleń warunkuje się zatwierdzeniem przez Zamawiającego harmonogramu szkoleń. Wykonawcę obowiązuje konieczność pisemnego zgłaszania Zamawiającemu każdorazowej zmiany harmonogramu z minimum dwudniowym wyprzedzeniem. Terminy szkoleń mogą ulec zmianie, wyłącznie na podstawie pisemnej zgody Zamawiającego. Potwierdzeniem wykonania szkoleń przez Wykonawcę będzie sporządzona przez Wykonawcę i podpisana przez każdego z użytkowników zestawu sprzętu komputerowego lista obecności wraz z potwierdzenie ilości godzin odbytego szkolenia.</td><td></td><td></td></tr>
<tr><td>10</td><td>Zasilacz awaryjny</td><td>
<table>
<tr><td>Lp.</td><td>Nazwa elementu, parametru lub cechy</td><td>Opis wymagań</td></tr>
<tr><td>1</td><td>Moc pozorna</td><td>1500 VA</td></tr>
<tr><td>2</td><td>Moc rzeczywista</td><td>1050 W</td></tr>
<tr><td>3</td><td>Topologia (klasyfikacja IEC 62040-3)</td><td>Line-interactive z AVR</td></tr>
<tr><td>4</td><td>Współczynnik mocy</td><td>0,9</td></tr>
<tr><td>5</td><td>Czas przełączenia na baterię</td><td><4 ms</td></tr>
<tr><td>6</td><td>Liczba, typ gniazd wyjściowych</td><td>8 x IEC C13</td></tr>
<tr><td>7</td><td>Typ gniazda wejściowego</td><td>IEC C20 16A</td></tr>
<tr><td>8</td><td>Czas podtrzymania dla 100% obciążenia dla pf=0,9</td><td>4 min</td></tr>
<tr><td>9</td><td>Czas podtrzymania przy 50% obciążenia dla pf=0,9</td><td>13 min</td></tr>
<tr><td>11</td><td>Napięcie znamionowe</td><td>220/230/240 V</td></tr>
<tr><td>12</td><td>Tolerancja napięci prostownika</td><td>184V - 276V</td></tr>
<tr><td>13</td><td>Częstotliwość znamionowa</td><td>50/60 Hz autodetekcja</td></tr>
<tr><td>14</td><td>Tolerancja częstotliwości</td><td>45– 55 Hz (sieć 50 Hz) 55 - 65 (sieć 60Hz)</td></tr>
<tr><td>15</td><td>Kształt napięcia</td><td>Sinusoidalny</td></tr>
<tr><td>16</td><td>Napięcie znamionowe wyjściowe</td><td>220/230/240 V do wyboru przez użytkownika</td></tr>
<tr><td>17</td><td>Zakres zmian napięcia</td><td>+6/-10% napięcia nominalnego</td></tr>
<tr><td>18</td><td>Częstotliwość wyjściowa</td><td>50/60 Hz</td></tr>
<tr><td>19</td><td>Współczynnik szczytu</td><td>3:1</td></tr>
<tr><td>20</td><td>Baterie wymieniane przez użytkownika "na gorąco"</td><td>Tak</td></tr>
<tr><td>21</td><td>Ochrona przed przeładowaniem</td><td>Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)</td></tr>
<tr><td>22</td><td>Ochrona przed głębokim rozładowaniem</td><td>Tak</td></tr>
</table>
</td><td></td><td>3 szt</td><td></td></tr>
</table>

			23	Okresowy automatyczny test baterii	Tak			
			24	System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.			
			26	Możliwość uruchomienia bez napięcia w sieci	Tak			
			27	Baterie wewnętrzne o pojemności nie mniejszej niż	9Ah 12V, minimum 2 szt.			
			28	Czas ładowania baterii do poziomu 90%	< 3 godz. do 90% pojemności użytkowej			
			29	Interfejs komunikacyjny	• USB			
					• RS232 DB-9 żeński (HID)			
					• port ROO oraz RPO			
			30	Panel sterowania z wyświetlaczem LCD	• Panel LCD. Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach.			
					• Poziomy rząd przycisków sterowania			
					• Poziomy rząd wskaźników stanu : zasialanie z siec(zielony), trybu bateryjnego (żółty), usterki (czerwony)			
					• Sygnalizator akustyczny			
			31	Sygnały akustyczne	• Awaria			
					• Niski stan naładowania baterii			
					• Przeciążenie			
					• Serwis			
			32	Przyciski sterujące i wskaźniki diodowe LED	• Przycisk Escape (anulowanie)			
					• Przyciski funkcyjne (przewijanie w górę i w dół)			
					• Przycisk Enter (potwierdzający)			
					• Przycisk ON/OFF załączenia i wyłączenia			
					• LED trybu zasilania z siec i(kolor zielony)			
					• LED trybu baterii (kolor żółty)			
					• LED usterki (kolor czerwony)			
			33	Kolor	Czarny RAL 9023 / RAL 9005			

		34	Typ obudowy	Uniwersalna Tower/Rack 2U			
		35	Wyposażenie standardowe	UPS, instrukcja obsługi(CD), instrukcja bezpieczeństwa			
				1 x kabel szeregowy RS-232,			
				1 x kabel komunikacyjny USB			
				2 x kable wyjściowe IEC 10A			
				2 x uchwyty kablowe			
				1 x zestaw szyn montażowych 19’			
				1x kabel wejściowy			
		38	Maksymalna szerokość	441 mm			
		39	Maksymalna wysokość	86,5 mm			
		40	Maksymalna głębokość	405 mm			
		41	Maksymalny ciężar	18 kg			
		42	Poziom hałasu w odl. 1m	do 45 dBA dla pracy normalnej			
		43	Znaki bezpieczeństwa	CE, IEC/EN 62040-1 (CB Report), IEC/EN 62040-2 class B			
		44	Gwarancja producenta	24 miesiące			
		45	Możliwość montażu ręcznego bypassu serwisowego	Tak			

Część II - Dostawa komputerów dla jednostek oświatowych

1.	Notebook	**Typ:** Komputer typu notebook z ekranem o przekątnej 15-16” i rozdzielczości nie mniejszej niż 1920 x 1080 pikseli (FullHD). Podświetlenie LED, matryca wykonana w technologii IPS lub EWV/VA. Jasność matrycy nie mniejsza niż 220 nitów. Kontrast nie mniejszy niż 500:1. Matryca z fabryczną powłoką przeciwodblaskową. Pokrywa matrycy wykonana z aluminium lub innego metalu w celu dodatkowego zabezpieczenia panelu LCD. **Procesor:** Procesor klasy x86, o min. 2 rdzeniach fizycznych/ 4 wątkach logicznych, zaprojektowany do pracy w komputerach przenośnych, taktowany nominalnym zegarem, co najmniej 2,6 GHz, z pamięcią cache co najmniej 4 MB, osiągający jednocześnie w teście PassMark Performance Test, co najmniej 3900 punktów w kategorii Average CPU Mark (wynik na dzień publikacji SWZ) i po raz pierwszy będący na wykresach PassMark „CPU First Seen on Charts” w latach 2020-2021. **Pamięć RAM:** DDR4 8 GB z możliwością rozbudowy do min. 32 GB z pełnym wsparciem dla pamięci działających z taktowaniem 3200MHz. Pamięć operacyjna/magazyn danych M.2 PCIe 256GB o parametrach odczyt/zapis 1200/1200MB/s. Możliwość dołożenia drugiego dysku pracującego w standardzie SATA	**17**	

		lub NVMe bez utraty gwarancji. **Karta graficzna:** Grafika zintegrowana z procesorem ze sprzętowym wsparciem dla DirectX 12, OpenGL 4.6. **Multimedia:** Karta dźwiękowa zgodna z HD Audio. Wbudowane głośniki. Kamera HD. Łączność Karta WLAN 802.11ac + BlueTooth 4.2. Zintegrowana gigabitowa karta LAN – zamawiający nie dopuszcza możliwości zastosowania karty USB-LAN. Bateria i zasilacz: Minimum 3 komorowa o pojemności 42Wh. Zasilacz dedykowany do notebooka -brandowany logo Producenta komputera. **Funkcje BIOS:** BIOS zgodny ze specyfikacją UEFI. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS bieżących informacji o: - numerze seryjnym komputera. - wersji BIOS. - ilości zainstalowanej pamięci RAM. - zastosowanym procesorze wraz z taktowaniem. - zamontowanym dysku twardym wraz z jego pojemnością i modelem.. Możliwość włączenia/wyłączenia zintegrowanego z komputerem touchpada. Możliwość włączenia/wyłączenia bezprzewodowej karty sieciowej i modułu BlueTooth. Możliwość włączenia/wyłączenia zintegrowanej karty LAN. Możliwość włączenia/wyłączenia karty dźwiękowej. Możliwość włączenia/wyłączenia zintegrowanej kamery. Możliwość włączenia/wyłączenia portów USB. Możliwość włączenia/wyłączenia modułu TPM. Możliwość ustawienia niezależnych haseł dla konta administratora, użytkownika i dysku twardego. Brak możliwości uruchomienia systemu operacyjnego bez podania hasła. Funkcja ustawień zależności między hasłem administratora a użytkownika tak, aby nie było możliwe wprowadzenie zmian z poziomu użytkownika bez podania hasła do konta administratora. Główne hasło zabezpieczające rozruch musi być zachowane nawet w przypadku odcięcia wszystkich źródeł zasilania (wliczając baterię RTC/CMOS).		
		Certyfikaty i standardy: CE dla oferowanego komputera. Oferowany laptop musi spełniać wymagania normy MIL-STD-810H lub normy równoważnej. ISO 9001:2015 dla autoryzowanego serwisu Producenta notebooka. **Waga i wymiary:** Waga nieprzekraczająca 1,75kg, wymiary maksymalne 36x24x1,95cm Bezpieczeństwo: Dedykowana dioda LED zintegrowanej kamery sygnalizująca pracę komponentu. Fizyczna przesłona na kamerze zintegrowana z obudową komputera. Zintegrowany z płytą główną moduł TPM Zintegrowane z obudową gniazdo Kensington		

		Wbudowany w obudowę czytnik linii papilarnych **Warunki gwarancji:** Minimum 36 miesięcy. Gwarancja realizowana na miejscu u klienta. Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych. Wymagana gwarancja na baterię Gwarancja na baterię nie może być krótsza niż gwarancja na całe urządzenie. W przypadku oferty, w której notebook posiada gwarancję 36 miesięcy, również bateria powinna być objęta takim samym czasem ochrony tj. 36 miesięcy. **Wsparcie techniczne producenta:** Możliwość sprawdzenia telefonicznego bezpośrednio u producenta oraz na stronie internetowej producenta oferowanego notebooka, po podaniu numeru seryjnego - konfiguracji sprzętowej notebooka oraz warunków gwarancji. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta notebooka, realizowany poprzez podanie na stronie internetowej producenta numeru seryjnego lub modelu notebooka **Porty** - 2 porty USB typ A (3.2 Gen 2) - 1 port USB typ A (2.0) - 1 port USB typ C (3.2 Gen 2) - 1 port HDMI - 1 port VGA - 1 port LAN RJ45 - 1 port Micro SD - 1 port audio 3.5mm jack (combo lub osobne łącza) Klawiatura Z dedykowanym blokiem numerycznym po prawej stronie, podświetlona. System operacyjny Windows 10 PRO lub równoważny Zamawiający dopuszcza licencję edukacyjną.		