Załącznik nr 5 do SWZ

Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest: **„Zakup systemów i urządzeń w celu podniesienia poziomu cyberbezpieczeństwa Starostwa Powiatowego w Bełchatowie i jednostek podległych". Zakup dokonywany w ramach Konkursu grantowego „Cyberbezpieczny Samorząd", priorytet II: zaawansowane usługi cyfrowe, działanie 2.2. – wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze europejskie na rozwój cyfrowy 2021-2027 (FERC)**

2. Charakterystyka przedmiotu zamówienia:

Zadanie 1: Switch'e oraz Access Point

1) 4 szt.: urządzenia typu switch o parametrach nie niższych niż:

Procesor	0.8 GHz
Pamięć Flash	256 MB
Pamięć RAM	512 MB
Przeznaczenie	Do szaf RACK 19"
Typ	Zarządzalny
Liczba portów LAN 10/100/1000	48 Sztuk
Podtyp:	10 Gigabit Ethernet
Porty:	48 x 10/100/1000 + 4 x 1 Gigabit / 10 Gigabit SFP+
Wykonanie:	Przepustowość: 130.95 Mpps Zdolność przełączania: 176 Gbps Opóźnienie (1 Gbps): 2.2 µs Opóźnienie (10 Gbps): 1.2 µs
Pojemność:	Routing table entries (static): 32
Zgodność z normami:	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.1ab (LLDP), IEEE 802.3az
Protokół routingu:	IGMPv2, IGMP, routing statyczny IPv4, MSTP, RSTP, STP
Protokół zdalnego zarządzania:	SNMP, RMON, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SCP, DHCP, IPv4, IPv6
Algorytm kodowania:	SSL
Metoda identyfikacji:	RADIUS
Cechy:	Sterowanie przepływem, obsługa DHCP, obsługa ARP, trunking, obsługa VLAN, auto-uplink (auto MDI/MDI-X), nasłuchiwanie IGMP, dublowanie portów, zarządzalność, obsługa IPv6, tryb półdupleksu, tryb pełnego dupleksu, obsługa protokołu Spanning Tree (STP), obsługa protokołu Rapid

	Spanning Tree (RSTP), obsługa protokołu Multiple Spanning Tree Protocol (MSTP), obsługa list dostępu (ACL), Quality of Service (QoS), obsługa Jumbo Frames, Trusted Platform Module (TPM), obsługa IPv4, obsługuje LACP, obsługuje LLDP, Link Aggregation Control Protocol (LACP), Class of Service (CoS), obsługuje SNMP, bufor pakietów 1,5MB, Bridge protocol data unit (BPDU), LLDP-MED, Green Ethernet (EEE)
Rozmiar tablicy adresów MAC	16000
Obsługiwane ramki Jumbo:	9216 bajtów
Prędkość magistrali wew.	176 Gb/s
Szybkość przekierowań pakietów	130.95 mpps
Obsługa VLANów	Tak
Zarządzalność	Tak
Możliwość instalacji w szafach 19’	Tak
Zasilacz:	Adapter mocy wewnętrznej
MTBF:	114 Lat
Zgodność z normami:	VCCI, CISPR 24, EN 61000-3-2, IEC 61000-3-2, IEC 61000-3-3, IEC 61000-4-11, IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, IEC 61000-4-8, EN 61000-3-3, UL 60950-1, IEC 60950-1, EN 60950-1, EN 60825-1, CNS 13438, EN 55024:2010, FCC CFR47 Part 15 A, ICES-003 issue 6 Class A, IEC 62368-1, UL 62368-1 Second Edition, CISPR 32 Class A, EN 62368-1:2014, CAN/CSA-C22.2 No. 60950-1, CISPR 35, EN 55035:2017, EN 55032:2015+AC:2016 Class A
	Urządzenie musi być przeznaczone na rynek Polski

2) 20 szt.: Urządzenia typu Switch o parametrach nie niższych niż:

Rodzaj urządzenia:	Przełącznik zarządzalny- 8 porty – smart
Porty:	8x10/100/1000
Wykonanie:	Czas oczekiwania (100Mbps): 5.2 Opóźnienie (1 Gbps): 2.8 Przepustowość: 11,9 Mp/s Zdolność przełączania: 16 Gb/s
Wielkość tablicy adresów MAC:	8000 wpisów
Obsługiwane ramki Jumbo:	9216 bajtów
Protokół routingu:	IGMPv2, IGMP

Protokół zdalnego zarządzania:	SNMP 1, SNMP 2c, HTTP, HTTPS, TFTP, SCP, ICMP
Algorytm kodowania:	SSL
Procesor:	800MHz
RAM:	512 MB SDRAM
Pamięć fleszowa:	256 MB
Wskaźniki statusu:	Status portu, tryb dupleksu portu, łącze/aktywność, prędkość
Cechy:	Sterowanie przepływem, automatyczne wykrywanie urządzenia, autonegocjacja, obsługa VLAN, automatyczna funkcja uplink (auto MDI/MDI-X), nasłuchiwanie IGMP, obsługa Syslog, dublowanie portów, możliwość aktualizacji firmwaru, obsługa SNTP, możliwość montowania na ścianie, obsługa protokołu Spanning Tree (STP), dziennik zdarzeń, Quality of Service (QoS), Trusted Platform Module (TPM), Cable Diagnostics Function, bez chłodzenia, obsługuje LLDP, klient DHCP, Class of Service (CoS), zarządzane w chmurze, bufor pakietów 1,5MB, Secure Copy (SCP), Link Aggregation, obsługa podwójnego obrazu, Denial of Service (DoS) protection, Green Ethernet (EEE), BPDU Filter, ochrona pętli, Global Storm Control, Port Scheduling
Zgodność z normami:	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.3ac, IEEE 802.1ab (LLDP), IEEE 802.3az
Interfejsy:	7 x 1000Base-T RJ-45 1 x 1000Base-T RJ-45 wejście PoE
Zasilacz:	Adapter mocy zewnętrznej
MTBF:	188.2 lata
Zgodność z normami:	IEC 61000-3-2, IEC 61000-3-3, EN 61000-3-3, ICES-003 Klasa A, CNS 13438 Class A, KN35, IEC/EN 61000-4-3, IEC/EN 61000-4-4, IEC/EN 61000-4-5, IEC/EN 61000-4-6, IEC/EN 61000-4-8, AS/NZS CISPR 32 Class A, KN32 Class A, IEC/EN 61000-4-11, IEC/EN 61000-4-2, EN 55032:2015, UL 62368-1 Second Edition, IEC/EN60950-1:2006 +A11:2009 +A1:2010 +A12:2011 +A2:2013, IEC/EN 60825-1:2014 Class 1, CISPR 32 Class A, EN 55035, CISPR 35, IEC 62368-1 Second Edition, CAN/CSA-C22.2 No. 62368-1 Third Edition, UL 62368-1 Third Edition, IEC 62368-1 Third Edition, CAN/CSA C22.2 No. 62368-1 Second Edition, FCC CFR47 Part 15 B Class A 2018
Produkt musi być przeznaczony na rynek Polski	

3) 1 szt. urządzenia tupu switch lub równoważny o parametrach nie niższych niż:

Typ	Zarządzalny Smart
Obudowa	Przeznaczona do montażu w szafie RACK 19”
Liczba portów	48 1000BASE-T Gigabit Ethernet
Obsługiwane warstwy	Layer 2, Layer 3
Interfejs zarządzania	Wiersz poleceń CLI, web GUI, port konsoli
Dodatkowe	SNMP, VLAN 802.1Q
Warunki gwarancji	Serwis urządzenia musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta

4) 1 szt.: urządzenia typu switch o parametrach nie niższych niż:

Montaż:	Możliwość instalacji w szafce 10”
Interfejs zarządzania:	Ethernet
Interfejs sieciowy:	16 portów GbE RJ45 w tym 8 portów PoE/PoE+ (Pins 1, 2+; 3, 6-)
Całkowita przepustowość:	16 Gb/s
Zdolność przełączania:	32 Gb/s
Zasilanie:	AC/DC, wewnętrzne
Maks. zużycie energii:	15W (z wyłączeniem wyjścia PoE)
Dostępne POE w sumie:	45 W
Max. POE wat na port według PSE PoE +:	30 W
Przyciski:	Resetowanie fabryczne
Certyfikaty:	CE, FCC, IC
Przełączanie warstwy 2:	• IGMP snooping • STP / RSTP with priorities and port-level disable • Port isolation • Storm control • Voice VLAN • Port mirroring • LACP port aggregation

	• Multicast / broadcast rate limiting • MAC address blocking • Flow control • 802.1X control • Jumbo frames • Proprietary loop protection • DHCP snooping / guarding • Egress rate limit • LLDP-MED • Port restricted by MAC • Device isolation with ACLs
Diody LED:	• System - status • Ethernet PoE - prędkość / łącza / aktywność • PoE - link / aktywność
Wymagania dotyczące aplikacji:	konsola centralnego zarządzania wspólna dla przełącznika oraz punktu dostępowego wskazanych w podpunkcie 4, 5, 6 niniejszego zadania

5) 3 szt.: urządzenia typu switch o parametrach nie niższych niż:

Interfejs zarządzania:	Ethernet
Interfejs sieciowy:	8 portów GbE RJ45 w tym 4 porty PoE/PoE+ (Pins 1, 2+; 3, 6-)
Całkowita przepustowość bez blokowania:	8 Gb/s
Zdolność przełączania:	16 Gb/s
Metoda zasilania:	54V DC, 1.1A zasilacz
Dostępne POE w sumie:	52 W
Max. POE wat na port według PSE PoE +:	30 W
Przyciski:	Resetowanie fabryczne
Certyfikaty:	CE, FCC, IC
Przełączanie warstwy 2:	• IGMP snooping • STP / RSTP with priorities and port-level disable • Port isolation • Storm control • Voice VLAN • Port mirroring • LACP port aggregation

	• Multicast / broadcast rate limiting • MAC address blocking • Flow control • 802.1X control • Jumbo frames • Proprietary loop protection • DHCP snooping / guarding • Egress rate limit • LLDP-MED • Port restricted by MAC • Device isolation with ACLs
Diody LED:	• System - status • Ethernet PoE - prędkość / łącza / aktywność • PoE - link / aktywność
Wymagania dotyczące aplikacji:	konsola centralnego zarządzania wspólna dla przełącznika oraz punktu dostępowego wskazanych w podpunkcie 4, 5, 6 niniejszego zadania

6) 1 szt. urządzenia typu Access Point lub równoważny o parametrach nie niższych niż:

Interfejsy sieciowe:	2 Gb porty Ethernet 10/100/1000
Przycisk:	Reset
Anteny:	3 anteny o podwójnej polaryzacji i zysku 3dBi
Standardy WiFi:	802.11 a/b/g/n/ac
Sposób zasilania:	Pasywne PoE (48V), 802.3af/803.2at
Zakres napięcia:	44-57 V DC
Zasilacz:	48V, 0.5A Gb PoE (w zestawie)
Moc nadawcza:	2.4 GHz: 22 dBm, 5 GHz: 22 dBm
BSSID:	4 na radio
Zabezpieczenia:	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
Certyfikaty:	CE, FCC, iC
Montowanie:	Na suficie / ścianie (uchwyt w zestawie)
Zaawansowane zarządzanie ruchem:	• VLAN 802.1Q • QoS Limit ustawiany na użytkownika • Izolowanie ruchu gości Wspierane • WMM Voice, Video, Best Effort, Background • Jednocześni klienci 200
Wpierane przepustowości (zależnie od modulacji / szerokości kanału)	• 802.11a 6, 9, 12, 18, 24, 36, 48, 54 Mb/s • 802.11n 6,5 - 450 Mb/s (MCS0 - MCS23, HT 20/40) • 802.11ac 6,5 - 1300 Mb/s (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80)

	• 802.11b • 802.11g	1, 2, 5.5, 11 Mb/s 6, 9, 12, 18, 24, 36, 48, 54 Mb/s
Wymagania dotyczące aplikacji:	konsola centralnego zarządzania wspólna dla przełącznika oraz punktu dostępowego wskazanych w podpunkcie 4, 5, 6 niniejszego zadania	

Zadanie 2: Urządzenie klasy UTM

1szt.: urządzenia klasy UTM (zawierającego zaawansowany Antywirus, audyt podatności i rozszerzony filtr URL) wraz z wdrożeniem o parametrach nie niższych niż:

Wydajność:	• Przepustowość Firewall (1518-bajtowa ramka danych) • Przepustowość IPS (1518-bajtowa ramka danych) • Przepustowość IPS (pliki HTTP 1 MB) • Przepustowość Antywirusa	4 Gbps 2 Gbps 1 Gbps 500 Mbps
VPN:	• Przepustowość IPSec - AES GCM • Maks. liczba tuneli IPSec VPN • Maks. liczba SSL VPN (tryb Portal) • Liczba jednoczesnych połączeń klientów SSL VPN	1 Gbps 100 50 50
Połączenia sieciowe:	• Liczba jednoczesnych sesji • Nowe sesje na sekundę • Maksymalna liczba bram głównych/zapasowych	300 000 20 000 64/64
Interfejsy sieciowe:	• Interfejsy Ethernet 100/1000/2500 • Interfejsy światłowodowe 1 Gb opcjonalny transceiver)	8 1 (poprzez
System:	• Maksymalna liczba reguł filtrowania • Maksymalna liczba tras statycznych • Maksymalna liczba tras dynamicznych	2 048/8 192 512 10 000
Redundancja:	• High Availability (Active/Passive) • Redundantne zasilanie	Tak Zewnętrzne
Sprzęt:	• Pamięć/Dysk lokalny • Pamięć lokalna (Log partition) • Help_outline • MTBF w 25°C (lata) • Wielkość urządzenia 19") • Wilgotność względna, podczas pracy (bez kondensacji) 90% @ 40°C • Układ TPM	Karta SD Tak 36,5 1U - (<1/2 20% do Tak
Serwisy:	• NGFW + IPS	

	• IPSec + SSL VPN • Audyt Podatności • Zaawansowany antywirus • Chmurowy filtr URL 65 kategorii • Antyspam
Certyfikacja:	• Zgodność CE/FCC/CB

Zamawiający wymaga:

1) Wdrożenia oferowanego sprzętu
2) Udokumentowanie minimum 10 lat doświadczenia w konfigurowaniu i wdrażaniu urządzeń systemu bezpieczeństwa UTM (Next Generation Firewall)
3) Udokumentowane minimum 5 lat doświadczenia w konfigurowaniu i wdrażaniu rozwiązań zaoferowanego producenta
4) Posiadanie przynajmniej jednego certyfikatu inżynierskiego wydanego przez producenta na najwyższym poziomie umożliwiającym rozwiązywanie problemów technicznych
5) Posiadanie przynajmniej jednego certyfikatu producenta na poziomie trenerskim
6) Udokumentowane co najmniej trzy sprzedaże rozwiązań klasy UTM o wartości minimum 100 tys zł brutto każda w okresie ostatnich 3 lat

Zadanie 3: Wsparcie dla UTM Watchguard

Wsparcie dla urządzeń UTM Watchguard – 5h do wykorzystania przez nielimitowany czas Możliwość skorzystania z pakietu wsparcia technicznego. W którego skład wsparcia wchodzi:

- Konsultacja telefoniczna z inżynierem technicznym,
- Możliwość wsparcia drogą mailową z technikiem lub za pomocą Chatu,
- 3 Certyfikowanych inżynierów watchguard (W tym jeden inżynier z certyfikatem trenerskim dla Watchguarda)
- Wymagany certyfikat ISO 9001

Zadanie 4: Serwery NAS

1) 1 szt.: Serwer NAS wraz z 4szt. dysków *10 TB HDD* o parametrach nie niższych niż:

Procesor:	4 rdzeniowy / 8 wątkowy w architekturze 64-bit x86
Pamięć systemowa:	Min. 8GB SODIMM DDR4 z możliwością rozbudowy do 64 GB
Pamięć flash:	5 GB (Ochrona systemu operacyjnego przed podwójnym rozruchem)
RAID:	0,1,5,6,10,50,60,JBOD,Single Disk
Zainstalowane dyski	Ilość: 4szt. Dedykowany do: zaproponowanego serwera NAS Rozmiar: 3.5” Typ: magnetyczny

	Pojemność: 10TB Wytrzymałość w czasie pracy: 65 G Wytrzymałość w czasie spoczynku: 250 G Niezawodność MTBF: 1000000h Prędkość obrotowa: 7200 obr./min. Pamięć cache: 256 MB Maks. Transfer zewnętrzny: 215 MB/s
Rodzaje wyjść / wejść:	USB 3.2 Gen. 2 – 3 szt. USB 3.2 Gen. 1 Type-C – 1 szt. RJ45(LAN) 2.5 Gbps – 2 szt. PCIe 3.0 x 4 – 2 szt.
Protokoły sieciowe:	AFP, Dynamiczny DNS (DDNS), HTTP, HTTPS. iPv4/iPv6, iSCSI, Serwer CIFS/SMB, Serwer DNS, Serwer DHCP, Serwer FTP, Serwer SFTP, Serwer NFS, Serwer VPN, S.M.A.R.T., SNMP, SSH, Telnet, VLAN (802.1Q), FTPS, TFTP, WebDAV, LDAP
System plików dla dysków zewnętrznych:	FAT32, exFAT, NTFS, NFS+, EXT3, EXT4
System plików:	EXT4
Zasilacz:	W zestawie
Dodatkowe informacje:	Funkcja Wake on LAN/WAN, Szyfrowanie woluminów
Dołączone akcesoria:	Zestaw montażowy, Kabel sieciowy – 1 szt., Kabel zasilający – 1 szt., Radiator dysku SSD M.2 – 2 szt.
Ramka zabezpieczająca:	Ramka Jumbo
Kieszenie na dyski:	2,5”/3,5” – 4szt.(Hot swap) M.2 PCIe NVMe 3.0 x 1 – 2szt.

Pozostałe Wymagane Parametry Sprzętowe:

- Obsługa przyspieszenia pamięci podręcznej SSD
- GPU pass-through
- Koprocesor arytmetyczny FPU
- Mechanizm szyfrowania (AES-NI)
- Obudowa: Typu Tower
- Możliwość rozbudowy o opcjonalne karty PCIe: wyjście HDMI, Port 5/10 Gigabit sieci ethernet, procesor graficzny, transkodowanie wspomagane sprzętowo
- Wskaźniki LED: Stan/zasilanie, USB, LAN, dyski 1–4, M.2 SSD 1–2
- Przyciski: zasilanie, reset, automatyczne kopiowanie USB
- Maks. liczba połączeń współbieżnych (CIFS) — z maks. pojemnością pamięci 200

• Zainstalowane dyski: 4 x 10 TB, 6Gb/s (SATA III) , znajdują się na liście kompatybilności producenta NAS-a przeznaczone do pracy ciągłej • NAS obsługuje oprogramowanie instalowane w postaci kontenerów Docker • Repozytorium dostępne w urządzeniu musi umożliwiać pobranie oraz instalacje wykorzystywanego w urzędzie oprogramowanie "FerroBackup" w formie kontenera Docker.

2) Dysk Sieciowy NAS o parametrach nie niższych niż:

Typ	Sieciowy serwer plików NAS
Obudowa	Wolnostojąca Miejsce na instalację min. 2szt. dysków twardych w rozmiarze 3,5''
Procesor	Procesor czterordzeniowy, osiągający w teście wydajności PassMark Average CPU Mark co najmniej 2900 punktów (wynik dostępny pod adresem https://www.cpubenchmark.net)
Pamięć RAM	Min. 2GB DDR4 RAM, z możliwością rozbudowy do 6GB.
Kontroler pamięci masowej	Obsługiwane typy dysków: SATA III, Obsługiwane tryby RAID min.: 0, 1.
Dyski twarde	3,5" 7200 RPM SATA III 4TB – 2 szt. - dedykowane do zaoferowanego NAS
Wbudowane porty	Min. 2 szt. min 1 GbE LAN RJ-45; min 1 port USB min 3.0
System operacyjny - funkcje	Wszystkie wymienione poniżej funkcjonalności zawarte są w cenie urządzenia, bez konieczności ponoszenia dodatkowych kosztów przez Zamawiającego. 1. Wbudowany serwer: CIFS/SMB 3.0, FTP, NFS, 2. Integracja z Microsoft Active Directory (AD).
Protokoły sieciowe	HTTPS, SMB, SMNP, FTP, SSH
Warunki gwarancji	Serwis urządzenia musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta.

Zadanie 5: <u>Usługa wdrożenia rozwiązania do centralnego składowania dzienników zdarzeń w opcji Open Source</u>

<u>1. Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń:</u>

1.1. System operacyjny powinien być na licencji Open Source.

1.2. Platformą sprzętowa dla rozwiązania centralnego składowania dzienników w sieci Zamawiającego będzie fizyczny serwer dostarczony przez i na koszt Wykonawcy o parametrach nie gorszych niż:

- Procesor: 2x (osiągający w teście wydajności PassMark Average CPU Mark co najmniej 15118 punktów (wynik dostępny pod adresem https://www.cpubenchmark.net))
- Pamięć RAM: 128GB
- Kontroler RAID: sprzętowy
- Dyski twarde: min 5TB(netto) w RAID 6
- Zasilanie: redundantne
- Interfejsy sieciowego: 4x GbE
- Obudowa: RACK z szynami do montażu w szafie teletechnicznej;
- Zarządzanie zdalne pozwalające na monitorowanie, obsługę i zarządzanie w każdym momencie jego pracy.

1.3. Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source
1.4. Tworzenie użytkowników w systemie centralnego składowania logów może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.
1.5. System centralnego składowania dzienników zdarzeń powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się m.in.: Sysloga UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514.
1.6. System centralnego składowania dzienników zdarzeń powinien mieć możliwość ekstrakcji fragmentów wpisów logów z możliwością wykorzystania ich do filtrowania danych, budowania zapytań dla powiadomień i alarmów czy widoków w ramach dashboardów oraz ich import jak i eksport.
1.7. System centralnego składowania dzienników zdarzeń powinien udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trypie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV czy urządzeniach z dowolną przeglądarką WWW.
1.8. System centralnego składowania dzienników zdarzeń powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego.
1.9. System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów).
2. W zakresie wdrożenia proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń:
2.1. Instalacja systemu operacyjnego na dostarczonym przez Wykonawcę serwerze fizycznym.
2.2. Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca zaproponuje rozwiązanie pozwalające na uspójnienie zegarów czasów sieci Zamawiającego.

2.3. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.
2.4. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktyw prawnych i dobrych praktyk występujących w środowisku Zamawiającego.
2.5. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:

- (1x) Urządzenie klasy UTM firmy WATCHGUARD
- (2x) Przełączniki zarządzalne firmy HP (48p)
- (3x) Przełączniki zarządzalne firmy Netgear (48p)
- (1x) Przełącznik zarządzalny firmy D-LINK (48p)
- (1x) Przełącznik zarządzalny firmy D-LINK (10p)
- (1x) Przełącznik zarządzalny firmy QNAP (16p)
- (4x) Przełączniki zarządzalne (48p)
- (20x) Przełączniki zarządzalne (8p)
- (4x) QNAP - Macierz dyskowa na dane
- (1x) Serwer Windows 2016 (2x HV na host)
- (2x) Serwer Windows 2019 (2x HV na host)
- (1x) Serwer Windows 2022 (1xHV na host)
- (2X) Serwer Windows 2022 (Migracja z 2016 w roku 2025)
- (2x) Serwer Linux (Ubuntu, Debian)
- (220) stacji roboczych Windows 10 i 11
- (1x) Aplikację Acronis Cyber Protect
- (1x) System Antywirusowy Bitdefender Gravity Zone
- (1x) Active Directory
- (1x) Serwer DNS
- (7x) Serwer wirtualizacji (HV)
- (2x) Serwer wirtualizacji (Linux)
- Inne aplikacje nie wymienione w spisie

2.6. Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.
2.7. Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.
2.8. Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.
2.9. Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.
2.10. Konfiguracja wysyłania powiadomień poprzez maila w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.
2.11. Wprowadzenie pracowników działu IT do obsługi wdrożonego systemu.
3. Szkolenie w formie warsztatu:

3.1. Zamawiający wymaga aby Wykonawca zorganizował i przeprowadził w swojej siedzibie lub innym miejscu nie zależnym od Zmawiającego warsztaty techniczne z zarządzenia i administracji wdrożonego systemu.
3.2. Zamawiający wymaga aby usługa została zrealizowana w terminie do 6 miesięcy od zamówienia usługi.
3.3. Zamawiający wymaga przeszkolenia w formie warsztatów 1 uczestnika.
3.4. Zamawiający wymaga aby w trakcie warsztatów realizowane były ćwiczenia opisujące codzienną pracę administracyjną z wdrożonym systemem, rozwiązywaniem problemów, procedurę aktualizacji rozwiązania oraz rozbudowy o dodatkowe widoki i kanały napływu danych.
3.5. Wymagana agenda warsztatów:
- Wstęp do zarządzania logami
- Wymagania oraz architektura wdrożonego rozwiązania
- Instalacja i konfiguracja ogólnych ustawień
- Zbieranie logów, czyli konfiguracja metod pozyskiwania dzienników zdarzeń.
- Przetwarzanie dzienników zdarzeń, czyli tworzenie strumieni logów, ich parsowanie oraz filtrowanie
- Wizualizacja logów czyli tworzenie czytelnych zestawień tabelarycznych i graficznych
- Konfiguracja alertów i powiadomień.
- Administracja i utrzymanie wdrożonego rozwiązania
- Case Study czyli praktyczne przykłady użycia

3.6. Zamawiający wymaga aby warsztaty zamykały się w ramach czasowych 2 dni roboczych (2x 7 godz.)
3.7. Zamawiający wymaga aby wykonawca pokrył koszty pełnego wyżywienia i zakwaterowania uczestnika w czasie warsztatów.
3.8. Zamawiający wymaga aby warsztaty kończyły się potwierdzeniem uczestnictwa w formie certyfikatu.

4. Gwarancja i asysta techniczne:

4.1. Zamawiający wymaga aby Wykonawca w czasie do 24 miesięcy od wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.
4.2. Zamawiający wymaga aby Wykonawca w okresie do 24 miesięcy od wdrożenia rozwiązania świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.
4.3. Zamawiający wymaga aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00.
4.4. Zamawiający akceptuje fakt, ze każda interwencja wymagać będzie od niego zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji będzie wyznaczony przez Wykonawcę, i może to być system zgłoszeń elektronicznych lub komunikacja mailowa.

5. Wymagania dotyczące doświadczenia wykonawcy:

5.1. Zamawiający wymaga aby Wykonawca w okresie ostatnich 12 miesięcy przed przystąpieniem do realizacji zadania był wstanie wykazać się minimum 5 wdrożeniami proponowanego rozwiązania w jednostkach publicznych o podobnej wielkości do Zamawiającego.

Zadanie 6: System do zarządzania infrastrukturą IT.

1. Architektura / budowa

1.1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 70 Klientów jednocześnie.

1.2. Architektura / budowa:

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

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

1.2.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.

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

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

1.3. Konfiguracja Architektury:

1.3.1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.

1.3.2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.

2. Wymagania systemowe

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

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

2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2

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

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

2.5. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych zarówno komercyjnych jak i bezpłatnych (np. Microsoft SQL Server Express Edition).

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

3. Interfejsy

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

3.2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL

3.3. System zapewnia integrację z modelem LLM.

4. Funkcjonalności systemu zarządzania infrastrukturą IT

4.1. Funkcjonalność Klienta

4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku.

4.2. Funkcjonalność konsoli administracyjnej.

4.2.1. Konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie.

4.2.2. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.

4.2.3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.

4.3. Funkcjonalność panelu pracownika

4.3.1. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.

4.4. Zarządzanie licencjami

4.4.1. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.

4.5. Wzorce aplikacji i pakietów

4.5.1. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.

4.6. Inwentaryzacja sprzętu komputerowego i urządzeń.

4.6.1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń.

4.7. Inwentaryzacja urządzeń sieciowych.

4.7.1. System musi posiadać zdolności do identyfikacji urządzeń sieciowych. Wymagane jest posiadanie skanera sieci i SNMP, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.

4.8. Inwentaryzacja sprzętu.

4.8.1. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.

4.9. Ochrona danych (DLP)

4.9.1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.

4.10. Zdalna administracja komputerami

4.10.1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.

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

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

4.13. Zdalne Zarządzanie Zaporą (Firewall)

4.13.1. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.

4.14. Automatyzacja

4.14.1. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.

4.15. Zarządzanie magazynem IT

4.15.1. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.

4.16. Repozytorium

4.16.1. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.

4.17. Kody kreskowe

4.17.1. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.

4.18. Wysyłanie wiadomości

4.18.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między administratorem a użytkownikami systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.

4.19. System musi posiadać możliwość eksportu / importu treści.

4.20. Monitorowanie drukarek sieciowych i wydruków

4.20.1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty

drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.

4.21. Monitorowanie stron www

4.21.1. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.

4.22. Monitorowanie serwerów WWW

4.22.1. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.

4.23. Monitorowanie dziennika zdarzeń

4.23.1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.

4.24. System musi umożliwiać monitorowanie komunikatów Syslog.

4.25. Monitorowanie pracy komputerów

4.25.1. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.

4.26. Monitorowanie sensorów

4.26.1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.

4.27. Repozytorium CMDB

4.27.1. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.

4.28. Worktime manager

4.28.1. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostepnienia w panelu pracownika.

4.29. Raportowanie i eksport danych

4.29.1. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym

miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.

4.30. System musi zapewnić interfejs API.

4.30.1. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.

4.31. Powiadomienia

4.31.1. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.

4.32. Bezpieczeństwo

4.32.1. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.

5. Wsparcie i pomoc

5.1.1. Pomoc techniczna

5.1.1.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.

5.1.1.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.

5.1.1.3. Czas trwania usługi SLA wynosi 12 miesięcy od dnia zakupu.

Zadanie 7: System do wykonywania backupu danych.

Czas trwania licencji – co najmniej 12 miesięcy.

1. Produkt i dokumentacja dostępna w polskiej (i angielskiej) wersji językowej
2. Wsparcie dla systemów operacyjnych Windows typu serwer:

Systemy operacyjne Windows:

- Windows Server 2016, 2019, 2022 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

Systemy operacyjne Linux:

System Linux z jądrem w wersjach od 2.6.9 do 6.9 i biblioteką glibc w wersji 2.3.4 lub nowszą, w tym następujące dystrybucje x86 and x86_64:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.0-8.8*, 9.0-9.4*

- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04, 22.10, 23.04, 23.10, 24.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 37, 38
- SUSE Linux Enterprise Server 10, 11, 12, 15
- SUSE Linux Enterprise Server 12 i 15 - obsługa w systemach plików, z wyjątkiem Btrfs
- Debian 4, 5, 6, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10.x, 11.x, 12
- CentOS 5.x, 6.x, 7.x, 8.x*
- CentOS Stream 8*,9*
- Oracle Linux 5.x, 6.x, 7.x, 8.x*,9.0-9.4* — wersje Unbreakable Enterprise Kernel i Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0-8.8*, 9.4*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.0 − 8.10*, 9.0 − 9.4*
- Rocky Linux 8.0 − 8.4*, 9.0 − 9.3*
- ALT Linux 7.0

3. Licencja dostępna w modelu subskrypcyjnym
4. Możliwość wdrożenia konsoli zarówno w trybie chmurowym jak i on-premis
5. Wsparcie i pełna funkcjonalność oprogramowania dla wielojęzykowych systemów operacyjnych
6. Obsługa środowiska chmurowego
7. Tworzenie kopii zapasowych dysków/partycji
8. Tworzenie kopii zapasowych plików i folderów
9. Replikacja kopii zapasowych do wielu lokalizacji docelowych
10. Tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
11. Kopie zapasowe i granularne przywracanie elementów aplikacji Microsoft Exchange, Microsoft SQL Server, Microsoft SharePoint i Microsoft Active Directory.
12. Możliwość przywrócenia kopii zapasowej dysku/partycji na innym komputerze o innej konfiguracji sprzętowej
13. Obsługa dysków twardych z sektorami o rozmiarze 4KB oraz dysków SSD
14. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
15. Zdalna instalacja i aktualizacja agentów na komputerach klienckich
16. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych oraz serwerach SFTP
17. Możliwość tworzenia niezmiennych magazynów przechowywania kopii zapasowych (tzw. immutable storage)
18. Możliwość generowania planu przywracania kopii zapasowych
19. Możliwość eksportu i importu planów tworzenia kopii zapasowych na różnych maszynach
20. Szablony schematów rotacji kopii zapasowych
21. Polecenia poprzedzające/następujące

22. Automatyczne usuwanie nieaktualnych kopii zapasowych (retencja)
23. Sprawdzanie poprawności i konsolidacja kopii zapasowych (pełnych, przyrostowych i różnicowych)

* Począwszy od wersji 8.4 obsługiwane tylko z jądrem w wersji od 4.18 i nowszej

24. Wykonywanie zadań i tworzenie kopii zapasowych możliwe z poziomu wiersza polecenia.
25. Możliwość utworzenia ukrytej partycji widzianej tylko przez oprogramowanie do backupu na potrzeby zapisu kopii zapasowych, która będzie chroniona za pomocą hasła
26. Współpraca z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
27. Pełne, przyrostowe i różnicowe kopie zapasowe
28. Wysyłanie powiadomień pocztą e-mail
29. Szyfrowane kopii zapasowych algorytmem AES
30. Tworzenie dynamicznych grup urządzeń na podstawie nazwy urządzenia, ilości pamięci operacyjnej, zakresu adresów IP, typu systemu operacyjnego
31. Możliwość wykonywania czynności przenoszenia kopii zapasowych, replikacji, weryfikacji i czyszczenia na innym systemie.
32. Funkcjonalność ciągłej ochrony danych
33. Wbudowany moduł ochrony antywirusowej. Środowisko Windows
34. Możliwość integracji z Windows Defender Antyvirus
35. Filtrowanie adresów URL
36. Analiza podatności urządzenia (poszukiwanie luk w oprogramowaniu objętym ochroną), środowisko Windows
37. Funkcjonalność zdalnego pulpitu, możliwa do wywołania z poziomu serwera zarządzania oprogramowaniem backupowym środowisko Windows
38. Moduł automatycznego łatania wykrytych luk w oprogramowaniu środowisko Windows
39. Automatyczne tworzenie kopii zapasowej urządzenia, na którym ma zostać wdrożona poprawką
40. Możliwość wywołania funkcji zdalnego wymazywania danych w oparciu o mechanizm wbudowany w Windowsa 10
41. Funkcja aktywnej ochrony przed oprogramowaniem ransomware, chroniąca pliki lokalne i pliki kopii zapasowych przed zaszyfrowaniem. (Środowisko Windows)
42. Predefiniowany schemat tworzenia kopii zapasowych: G-F-S
43. Priorytetowe przywracanie systemu operacyjnego - Jeśli system uległ awarii, można go uruchomić w ciągu kilku sekund, a proces przywracania będzie wykonywany w tle.
44. Uruchamianie usług z minimalnymi prawami użytkownika
45. Zaawansowane raportowanie - możliwość tworzenia raportów w oparciu o predefiniowane schematy
46. Pomoc techniczna dostępna w języku polskim
47. Administrowanie kontami użytkowników Acronis i jednostkami organizacyjnymi
48. Tworzenie kryptograficznego odcisku pliku (sumy kontrolnej) wykorzystującego technologię blockchain
49. Wykonywanie kopii zapasowych uruchamiane po wystąpieniu określonych zdarzeń i warunków

50. Migawki wielowoluminowe
51. Kopia zapasowa „sektor po sektorze"
52. Obsługa dysków dynamicznych
53. Automatyczne ponawianie prób w przypadku niekrytycznych błędów (prób utworzenia kopii zapasowej)
54. Możliwość utworzenia nośnika startowego opartego na środowisku Linux lub WinPE