

Załącznik nr 3 do Zapytania ofertowego

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Część nr.1

Urządzenie brzegowe UTM – wraz z niezbędną aktualizacją

Dostarczenie maszyna wirtualna typu firewall spełniająca następujące funkcjonalności:

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPsec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPsec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.8 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
 - Amazon Web Services (AWS).
 - Microsoft Azure
 - Cisco ACI.
 - Google Cloud Platform (GCP).
 - OpenStack.
 - VMware vCenter (ESXi).

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPsec VPN. W zakresie tej funkcji musi zapewniać:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługa protokołu Diffie-Hellman grup 19 i 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Obsługa mechanizmów: IPsec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
 - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
 - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
 - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec VPN lub SSL VPN.

Routing i obsługa łącz WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
 - Routingu statycznego.
 - Policy Based Routingu.
 - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
 - Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Hasel dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
1. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
3. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

- a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [12] miesięcy.

Gwarancja oraz wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres [12] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Część nr.2

Zakup urządzeń podtrzymujących napięcie – UPS – serwerownia.

Urządzenie zapewniające wydajną ochronę zasilania systemów i danych, a tym samym zapewniają niezawodną ochronę przed awariami zasilania, wahaniami prądu i zakłóceniami elektrycznymi.

Wymagania ogólne:

Moc wyjściowa (pozorna / czynna) - minimum 3000 VA, minimum 3000 W

Topologia - VI (line interactive)

Typ obudowy- Rack / Tower

Chłodzenie - Wymuszone, wewnętrzne wentylatory

Napięcie znamionowe (wartość skuteczna) - 230 V AC

Zakres napięcia wejściowego (wartości skuteczne) i tolerancja - 178 ÷ 281 V AC ± 2 %

Częstotliwość znamionowa napięcia wejściowego - 50 Hz

Zakres częstotliwości i tolerancja - 45 ÷ 55 Hz ± 1 Hz

Progi przełączania: sieć – UPS - 178 ÷ 281 V AC ± 2 %

Napięcie znamionowe (wartość skuteczna) - 230 V AC

Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa - 195 ÷ 253 V AC ± 2 %

Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca rezerwowa - 230 V AC ± 5 %

Automatyczna regulacja napięcia (AVR) - ± 10 %

Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej) - Sinusoidalny / Tak jak na wejściu

Częstotliwość znamionowa napięcia wyjściowego - 50 Hz

Filtracja napięcia wyjściowego - Filtr przeciwzakłóceń RFI/EMI, tłumik warystorowy

Progi przełączania: UPS – sieć - 183 ÷ 276 V AC ± 2 %

Czas przełączenia na pracę rezerwową - < 3 ms

Czas powrotu na pracę sieciową - 0 ms

Przebieżalność - > 105% - 15 s (wyłączenie UPS)

Akumulatory wewnętrzne - minimum 12 V / 7 Ah VRLA

Możliwość podpięcia modułów bateryjnych wymagane - minimum 1szt

Czas podtrzymania z baterii wewnętrznych (80 % / 50 % Pmax) - minimum 4 / 7 min

Maksymalny czas ładowania baterii wewnętrznych UPS do 90% pojemności baterii - po uprzednim rozładowaniu obciążeniem równym 80% Pmax (do wyłączenia się zasilacza) - do 4 h

Wymiary – Rack (wys. X szer. X gł.) - nie większe niż 132 x 440 x 630 mm

Masa zasilacza - nie większa niż 43 kg

Zabezpieczenie wejściowe - Przeciwzwarceniowe – Bezpiecznik automatyczny 16 A / 250 V AC, Przeciwpzepięciowe.

Zabezpieczenie wyjściowe - Elektroniczne – przeciwzwarceniowe i przeciążeniowe

Zabezpieczenia wejścia DC (akumulatory wewnętrzne) - Zabezpieczenie nadprądowe

Zabezpieczenia DC (zewnętrzny moduł bateryjny) - Zabezpieczenie nadprądowe

Przylączy wyjściowe (liczba i typ gniazd) - minimum 9 gniazd z podtrzymaniem baterijnym (w tym minimum 2 gniazda w standardzie PL z bolcem uziemiającym)

Sygnalizacja - Akustycznie – optyczna; graficzny wyświetlacz LCD

Interfejsy komunikacyjne - USB HID, SNMP/HTTP

Filtr teleinformatyczny (linii danych) – RJ45 - LAN 1 Gbit/s

Wsporniki do montażu w szafie RACK - wymagane

Oprogramowanie monitorująco-zarządzające - oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS, możliwość zdalnego włączenia / wyłączenia UPSa (poprzez SNMP), możliwość zdalnego wyłączenia zarządzanej sekcji gniazd, możliwość edycji nazw urządzeń na liście monitorowanych UPSów, wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów, wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer.

Możliwość ustawienie minimalnego stopnia naładowania akumulatorów, przy którym zasilacz uruchomi się po rozładowaniu akumulatorów i powrocie napięcia sieciowego - wymagane

Możliwość aktualizacji oprogramowania firmware przez użytkownika - wymagane

Deklaracje - CE

Normy - PN-EN 62040-1:2009, PN-EN 62040-2:2008

Gwarancja - min 36 miesięcy na elektronikę i 36 miesiące na akumulatory;

Serwis - autoryzowany serwis producenta zlokalizowany w Polsce, serwis realizowany w systemie door to door.

DODATKOWE OŚWIADCZENIA/DOKUMENTY - ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania - należy dołączyć do oferty dokument potwierdzający spełnienie wymagań, jeżeli oferowana jest niestandardowa, rozszerzona gwarancja to wymagane jest by realizowana była wyłącznie przez serwis producenta - należy przedstawić odpowiednie oświadczenie producenta, oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji, karta katalogowa oferowanego sprzętu.

Część nr.3

Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.

Zamawiający wymaga, aby wszystkie dostarczone urządzenia zostały umieszczone (zamontowane) i uruchomione we wskazanych przez Zamawiającego miejscach przeznaczenia, w uzgodnionym przez obie strony terminie. Sposób montażu sprzętu ma być dostosowany do technologii wykonania oraz ma być przeprowadzony zgodnie z zaleceniami producenta.

Część nr.4

Router - Switche

Dostarczone urządzenie musi spełniająca następujące funkcjonalności:

Wymagania Ogólne

Porty przełącznika: minimum 52x 10/100/1000Base-T RJ45 oraz minimum 4x 1/10GBase-X SFP+

Port konsolowy: RJ45 (RS-232)

Port USB: minimum 1 port co najmniej w standardzie 2.0

Szybkość przełączania: minimum 176Gb/s

Przepustowość: minimum 130Mp/s (dla pakietów 64Kb)

Bufor pakietów: minimum 1,5 MB

Ramki Jumbo: minimum 10k

Tablica adresów MAC: minimum 16k

Adresy MAC – Multicast: minimum 1k

Tablica ACL: minimum 512

Tablica VLAN: minimum 4094

Taktowanie procesora: minimum 800MHz

Pamięć Flash: minimum 32MB

Pamięć RAM: minimum 256MB

Temperatura pracy: zakres minimum 0°C - 50°C

Wilgotność względna: zakres minimum 10% - 90% (bez kondensacji)

Zasilanie: zabudowany zasilacz 230V AC

Pobór mocy: maksymalnie 50W

Zabezpieczenie przeciwprzepięciowe: minimum 6kV

Wymiary: maksymalna: szerokość 440 mm, wysokość 44mm , głębokość 280mm

Certyfikaty bezpieczeństwa: CE, RoHS

Algorytm: Store and Forward

VLAN: Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ

DHCP: IPv4/IPv6 DHCP Client, IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP

Snooping, IPv4/IPv6 DHCP Server

Spanning tree: IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding

Protekcja ringowa: ITU-T G.8032 – recovery time < 50ms, Fast Link, Loopback Detection

Agregacja łączy: IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balance

Bezpieczeństwo: Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,

Multicast: IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication

QoS: 8 queues per port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI

Mark/Remark, IEEE 802.1p, Queuing Method: Strict Priority, Weighted Deficit Round Robin, Strict priority in Weighted Deficit Round Robin; DNS Client, DNS Relay

Lista kontroli dostępu: IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN

Diagnostyka: sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route, Dying GASP

Zarządzanie: TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (4 devices in one stack) – hardware stacking

Oprogramowanie oraz wsparcie techniczne: oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług

Gwarancja: lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.

Część nr. 5

Serwer wraz z oprogramowaniem Windows Serwer i szafy typu rack

Wymagania ogólne:

Obudowa - Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.

Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.

Płyta główna - Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

Chipset - Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

Procesor - Zainstalowany jeden procesor min. 16-rdzeniowy, min. 2.4GHz, klasy x86 dedykowany do pracy z zaferowanym serwerem umożliwiający osiągnięcie wyniku min. 229 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. Możliwość obsługi procesorów 32 rdzeniowych

RAM - Minimum 32GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.

Funkcjonalność pamięci RAM - Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing

Gniazda PCI - minimum jeden slot PCIe x16 generacji 4

Interfejsy sieciowe/FC/SAS - Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

Dyski twarde - Zainstalowane 2 dyski SSD SATA o pojemności min. 1.92TB, 2,5" Hot-Plug. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.

Kontroler RAID - Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10

System operacyjny/System wirtualizacji - Microsoft Windows Server 2022 Standard

Dodatkowo należy dostarczyć:

- nośnik CD/DVD umożliwiający downgrade do wersji Windows Server 2019 Standard

Wbudowane porty - 4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim.

Video - Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200

Zasilacze - Redundantne, Hot-Plug min. 800W każdy.

Bezpieczeństwo - • Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej.

- Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
- BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
- Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
- Moduł TPM 2.0
- Możliwość dynamicznego włączania i wyłączenia portów USB na obudowie – bez potrzeby restartu serwera
- Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem

Diagnostyka - Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.

Karta Zarządzania - Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:

- zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
- zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
- szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;
- możliwość podmontowania zdalnych wirtualnych napędów;
- wirtualną konsolę z dostępem do myszy, klawiatury;
- wsparcie dla IPv6;
- wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
- integracja z Active Directory;
- możliwość obsługi przez dwóch administratorów jednocześnie;
- wsparcie dla dynamic DNS;
- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
- możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
- możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera

Oprogramowanie do zarządzania - Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:

- Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
- integracja z Active Directory
- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
- Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
- Szczegółowy opis wykrytych systemów oraz ich komponentów
- Możliwość eksportu raportu do CSV, HTML, XLS, PDF
- Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
- Grupowanie urządzeń w oparciu o kryteria użytkownika
- Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
- Szybki podgląd stanu środowiska
- Podsumowanie stanu dla każdego urządzenia
- Szczegółowy status urządzenia/elementu/komponentu
- Generowanie alertów przy zmianie stanu urządzenia.
- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
- Integracja z service desk producenta dostarczonej platformy sprzętowej
- Możliwość przejęcia zdalnego pulpitu
- Możliwość podmontowania wirtualnego napędu
- Kreator umożliwiający dostosowanie akcji dla wybranych alertów
- Możliwość importu plików MIB
- Przesyłanie alertów „as-is” do innych konsol firm trzecich
- Możliwość definiowania ról administratorów
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
- Wdrażanie serwerów, rozwiązań modułowych oraz przełączników sieciowych w oparciu o profile
- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.

- Zdalne uruchamianie diagnostyki serwera.
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

Certyfikaty - Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001

Serwer musi posiadać deklaracja CE.

Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.

Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.

Dokumentacja użytkownika - Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Warunki gwarancji - 3 lata gwarancji producenta

Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.

Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.

Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.

Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.

Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.

Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.

Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.

Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.

Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.

Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

Możliwość rozszerzenia gwarancji przez producenta do 7 lat.

Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

Szafa rack

Wymagania ogólne

Konstrukcja

Drzwi przednie wyposażone są w zamek powtarzalny, zapobiegający przypadkowemu dostępowi do zawartości szafy przez osoby niepowołane. **Szyba** jest wykonana z wysokiej jakości **szkła hartowanego** o zwiększonej odporności na naprężenia mechaniczne i zmiany temperatury. Osłony boczne posiadają zatrzaski ułatwiające ich demontaż. Opcjonalnie mogą zostać wyposażone w zamki. Elementy szafy są **malowane proszkowo na kolor czarny**.

Wyposażenie

W standardowym wyposażeniu szafy znajduje się podsufitowy **panel wentylacyjny, dwie półki stałe** mocowane czteropunktowo, zespół jezdy w postaci 4 kół oraz **listwa zasilająca** z uziemieniem. Szafa jest dostarczana w 3 kartonach w formie wygodnego **zestawu do samodzielnego montażu**, który ułatwia wnoszenie nawet do trudnodostępnych pomieszczeń.

Cechy produktu:

- wysokość z kółkami: 856mm
- wysokość bez kółek: 789mm
- wytrzymała konstrukcja
- łatwość montażu
- panel wentylacyjny z czterema wentylatorami

- listwa zasilająca z wyłącznikiem (8 gniazd)
- dostarczana w 3 paczkach ułatwiających transport
- stopki i zestaw jezdny w zestawie
- malowanie proszkowe
- kolor czarny

Standard (cale) - 19"

Wysokość (U) - 15U ($\approx 770/860\text{mm}$)

Szerokość - 600mm

Głębokość - 1000mm

Rodzaj - stojąca

Drzwi przednie - szyba, z zamkiem

Oslony boczne - demontowalne, możliwość montażu zamka, stalowe, zamykane na zatrzask

Tył - drzwi, stal

Belki - rackowe 4x regulowane

Przepusty kablowe - góra i dół

Wyposażenie - 1x listwa zasilająca, 2x półka stała, panel wentylacyjny 2 wentylatory

Informacje dodatkowe - dostarczana w 3 kartonach

Dopuszczalne obciążenie - do 300kg

Wymiary - 600x1000x856mm (SxGxW)

Waga - 43kg

Kolor - czarny

Część nr.6

Urządzenie do robienia backupów NAS wraz z 4 dyskami 12TB

Wymagania ogólne:

Procesor - Intel® Celeron® N5105/N5095 4-core/4-thread processor, burst up to 2.9 GHz

Obudowa - Rack 2U o wymiarach, 88,6 × 482,14 × 346,43 mm

(wys. x szer. x gł.) wraz z szynami umożliwiającymi montaż w szafie rack

Pamięć RAM - 4 GB SO-DIMM DDR4 (1 x 4 GB)

Ilość obsługiwanych dysków - 8 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s

Dyski - 4 dyski 3,5-cala HDD, min. 12TB SATA, 7200RPM, 256MB cache, min. 2,5 mln MTBF, przeznaczony do pracy 24/7, serii Enterprise, gwarancja producenta 60 miesięcy

Interfejsy sieciowe - 2 porty 2,5 Gigabit sieci Ethernet (2,5G/1G/100M) obsługa VLAN i Jumbo Frame.

Porty - 2x USB 2.0, 2x USB 3.2 Gen 2, 1x HDMI 1.4b

Wskaźniki LED - HDD 1–8, stan, LAN, rozszerzenie, zasilanie

Obsługa RAID - Pojedynczy dysk, JBOD, RAID 0,1,5,5+Spare,6,6+Spare,10 i 10+Spare, RAID50, RAID60. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk.

Funkcje RAID - Możliwość zwiększania pojemności i migracja między poziomami RAID online.

Szyfrowanie - Możliwość szyfrowania całych woluminów kluczem AES 256 bitów.

System Operacyjny - Apple Mac OS 10.10 or later Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 or later Linux IBM AIX 7, Solaris 10 or later UNIX Microsoft Windows 7, 8, and 10 Microsoft Windows Server 2008 R2, 2012, 2012 R2 and 2016, 2019

Stacja monitoringu - Obsługa do 24 kamer IP (8 licencji domyślnie).

Protokoły - CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP

Usługi - Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk

umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog, Virtualization Station

Zarządzanie dyskami - SMART, sprawdzanie złych sektorów

Język GUI – Polski

Gwarancja i serwis - 36 miesięcy, producenta

Waga - 10,47 kg (brutto), 7,9kg (netto)

Pobór mocy - Uśpienie: 31.742 W Praca: 55.83 W

System plików - Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+

Liczba kont użytkowników - 4096

Liczba grup – 512

Liczba udziałów – 512

Max ilość połączeń (CIFS) – 1500

Max liczba migawek – 1024

Zasilanie - 300 W, 100–240 V

Wentylator - 80mm, 12VDC

UPS - Obsługa sieciowych awaryjnych zasilaczy UPS.

Dyski twarde 4 sztuki o pojemności 12TB

Wymagania ogólne dysku:

Pojemność - 12 TB

Interfejs - SAS

Disk Speed (RPM) - 7200rpm

Cache Size (MB) - 356MB

Wymiary (L x W x H) - 147mm x 101.6mm x 26.1mm

Część nr.7

Oprogramowanie do Backup (kopi zapasowych)

Wymagania ogólne:

Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej

Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.

Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej

Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków

Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-incremental)

Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji

Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.

Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.

Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Google Cloud Storage, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane.

Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.

Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania

Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.

Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)

Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu

Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API

Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji

Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji

Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania

Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)

Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

Wymagania RPO

Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej

Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczeniu udziałów plikowych.

Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych

Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru

Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora

Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych.

Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, INFINIDAT, Pure Storage.

Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.

Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn

Oprogramowanie musi posiadać wsparcie dla NDMP

Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)

Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.

Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.

Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.

Repozytoria oparte o XFS muszą pozwalać na zmienność danych przez określoną ilość czasu (tzw Immutability)

Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.

Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.

Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik

Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)

Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

Wymagania RTO

Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.

Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)

Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami

Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków

Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików

Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.

Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:

- o Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
- o BSD: UFS, UFS2

- o Solaris: ZFS, UFS
- o Mac: HFS, HFS+
- o Windows: NTFS, FAT, FAT32, ReFS
- o Novell OES: NSS

Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.

Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.

Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),

Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych

Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych

Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.

Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA

Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Ograniczenie ryzyka

Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.

Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.

Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem

Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere

Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.

Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

Monitoring

System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich

System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie

System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.

System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware

System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter

System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn

System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel

System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk

System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora

System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów

System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)

System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna

System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego

System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta

System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.

System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware

System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 9.5 do 10.3

Raportowanie

System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022

System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.

System musi być certyfikowany przez VMware i posiadać status „VMware Ready”

System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V

System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF

System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc

System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach



Część nr.8

Patch panel rack – 2 sztuki

Urządzenie sieciowe służące do zakończenia kabli skrętkowych prowadzonych w okablowaniu.

Wymagania ogólne

24-portowy **nieekranowany patch panel kategorii 5e** o wysokości 1U, zaprojektowany do montażu w szafach rack 19".

Cechy produktu:

- 24-porty RJ-45
- klasa D (kat.5e)
- montaż w szafach rack 19"
- nieekranowany
- półka do organizowania kabli
- kolor czarny

Część nr 9

Stacje robocze – 10 sztuk

Komputery stacjonarne wraz z monitorami, klawiaturami oraz myszkami o minimalnych wymaganiach:

Wymagania ogólne:

Typ - Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.

Zastosowanie- Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.

Procesor - Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 13 800 punktów na dzień 6.06.2023.

Pamięć RAM - 8 GB DDR4 3200 MHz non-ECC możliwość rozbudowy do min 64GB, min. 1 slot wolny.

Pamięć masowa - SSD 256GB M.2 NVMe PCIe

Napęd optyczny - Nagrywarka DVD +/-RW o prędkości min. 8x

Grafika - Zintegrowana karta graficzna

Wyposażenie multimedialne - Karta dźwiękowa zintegrowana z płytą główną, port audio combo (słuchawki + mikrofon)na panelu przednim, na tylnym audio out.

Obudowa - Typu SFF z obsługą kart rozszerzeń o niskim profilu, napęd optyczny w dedykowanej wnęcie zewnętrznej slim. Suma wymiarów mierzona po krawędziach obudowy nie może przekraczać 678 mm, waga max 6kg,

Zasilacz o mocy max. 180W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 81% przy obciążeniu zasilacza na poziomie 100%,

Wbudowany w zasilaczu system diagnostyczny do sprawdzenia zasilacza bez konieczności włączania komputera, zasilacz w oferowanym komputerze musi się znajdować na stronie <http://www.plugloadsolutions.com/80pluspowersupplies.aspx>, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus, w przypadku, kiedy u producenta występuje kilka zasilaczy, które są montowane na etapie produkcji w fabryce załączyć wydruki dla wszystkich zasilaczy.

Wydruki 80plus muszą być potwierdzone przez producenta lub dołączone oświadczenie producenta komputera iż wskazane zasilacze przez wykonawcę spełniają 80plus.

Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED np. przycisku POWER [tzn. barw i miganie] W szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię procesora.

Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wnek zewnętrznych oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego.

Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz musi być wpisany na stałe w BIOS.

Zgodność z systemem operacyjnym - Potwierdzenie kompatybilności komputera na daną platformę systemową (wydruk ze strony)

Bezpieczeństwo - Ukryty w laminacie płyty głównej 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. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej.

System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. Działający w pełni, bez okrojonych funkcjonalności nawet w przypadku uszkodzonego dysku, braku dysku lub sformatowanym dysku, dostępu do sieci i internetu oraz bez konieczności podłączenia urządzeń wewnętrznych i zewnętrznych oraz bez konieczności pobierania i instalowania np. na ukrytej pamięci flash BIOS.

BIOS - BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, nazwę producenta komputera, model komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy.

Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych oraz dodatkowego oprogramowania typu system diagnostyczny odczytania z wewnętrznego menu BIOS informacji o: wersji BIOS, nr seryjnym komputera, dacie wyprodukowania komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, obecnej, minimalnej i maksymalnej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardego, MAC adresie zintegrowanej karty sieciowej, 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 ustawienia hasła systemowego/użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym hasle administratora.

Możliwość wyłączenia portów USB w tym:

- tylko portów USB znajdujących się na przednim panelu obudowy,
- tylko portów USB znajdujących się na tylnym panelu obudowy.
- wszystkich portów USB
- pojedynczo

Warunki gwarancji - 3-letnia gwarancja producenta świadczona na miejscu u klienta, Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.

Wsparcie techniczne producenta - Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony.

System Operacyjny - Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny musi być zapisany trwale w BIOS.

Porty I/O - Wbudowane porty:

- panel przedni : 2x USB 3.2 gen 1, 2x USB 2.0, 1x audio (dopuszcza się combo),
- panel tylny: 1x audio out, 2x USB 3.2 gen 1, 2x USB 2.0, 1x DP 1.4, 1x HDMI 1.4b, 1x RJ45

Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w : 1x PCI Express x16, 1x PCI Express x1, min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 2 złącza SATA w tym 1 szt SATA 3.0, 1 złącze M.2 dla dysków SSD, 1 złącze M.2 dla bezprzewodowej karty WiFi.

Wymagania dodatkowe - Klawiatura USB w układzie polski programisty

Mysz USB z klawiszami oraz rolką (scroll)

Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.

Dodatkowe oprogramowanie - Dołączone do oferowanego komputera oprogramowanie z nieograniczoną licencją czasowo na użytkowanie umożliwiające :

- upgrade i instalacje wszystkich sterowników, aplikacje dostarczone w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,
- możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS'u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :

- a. o poprawkach i usprawnieniach dotyczących aktualizacji
- b. dacie wydania ostatniej aktualizacji
- c. priorytecie aktualizacji
- d. zgodność z systemami operacyjnymi
- e. jakiego komponentu sprzętu dotyczy aktualizacja
- f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.

- wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne

- możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.

- rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)

- sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania)

- dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml
- raport uwzględniający informacje o : sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml od razu spakowany z rozszerzeniem *.zip. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.

Monitor

Typ ekranu - Ekran ciekłokrystaliczny z aktywną matrycą min. 23,8" (16:9)

Rozmiar plamki - 0,274 mm

Jasność - 250 cd/m²

Kontrast - Typowy 3000:1

Czas reakcji matrycy - max 5ms (Gray to Gray)

Rozdzielczość maksymalna - 1920 x 1080 przy 60Hz

Częstotliwość odświeżania poziomego - 30 – 83 kHz

Częstotliwość odświeżania pionowego - 48 – 75 Hz

Color Gamut - 72% (CIE 1931)

Zużycie energii - Normalne działanie 15,7 W (typowe), 24W (maksymalne), tryb wyłączenia aktywności mniej niż 0,4W

Powłoka powierzchni ekranu - Antyodblaskowa utwardzona

Podświetlenie - System podświetlenia LED

Bezpieczeństwo - Monitor musi być wyposażony w tzw. Kensington Slot - gniazdo zabezpieczenia przed kradzieżą.

Wbudowane w monitor narzędzie diagnostyczne umożliwiające zdiagnozowanie problemu wyświetlania obrazu na ekranie (kwestia karty graficznej czy monitora)

Waga bez podstawy - Maksymalnie 3,18 kg

Waga z podstawą + kable - Maksymalnie 3,51 kg

Wymiary bez podstawy - Wysokość : max. 332 mm

Szerokość : max. 553 mm

Głębokość : max. 50 mm

Wymiary z podstawą - Wysokość : max. 421 mm

Szerokość : max. 553 mm

Głębokość : max. 179 mm

Zakres regulacji Tilt - Wymagany, od -5 do +21 lub min. regulacja 26 stopni

Kolor obudowy – czarny

Złącze - 1x 15-stykowe złącze D-Sub, 1 x HDMI 1.4

Gwarancja - 5 lata na miejscu u klienta

Czas reakcji serwisu - do końca następnego dnia roboczego

Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta– dokumenty potwierdzające załączyć do oferty.

Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.

Certyfikaty - ISO 13406-2 lub ISO 9241, CE

Wymagane dokumenty dołączyć do oferty dodatkowo potwierdzone przez producenta sprzętu oświadczeniem lub podpisane przez osobę upoważnioną/prokurenta do reprezentowania producenta sprzętu.

Inne - Zdejmowana podstawa oraz otwory montażowe w obudowie VESA 100mm

Możliwość podłączenia do obudowy dedykowanych głośników producenta monitora

Typ ekranu Ekran ciekłokrystaliczny z aktywną matrycą min. 21,45” (16:9)

Rozstaw pikseli 0,249x0,241mm

Jasność 250 cd/m²

Kontrast Typowy 3000:1

Czas reakcji matrycy max 5ms (Gray to Gray)

Rozdzielczość maksymalna 1920 x 1080 przy 60Hz

Color Gamut 72% (CIE 1931)

Zużycie energii Normalne działanie 14,1 W (typowe), 22W (maksymalne), tryb wyłączenia aktywności mniej niż 0,3W

Powłoka powierzchni ekranu Antyodblaskowa utwardzona

Podświetlenie System podświetlenia LED

Bezpieczeństwo Monitor musi być wyposażony w tzw. Kensington Slot - gniazdo zabezpieczenia przed kradzieżą.

Wbudowane w monitor narzędzie diagnostyczne umożliwiające zdiagnozowanie problemu wyświetlania obrazu na ekranie (kwestia karty graficznej czy monitora)

Waga bez podstawy Maksymalnie 2,5 kg

Waga z podstawą + kable Maksymalnie 3 kg

Wymiary bez podstawy Wysokość : max. 332 mm

Szerokość : max. 553 mm

Głębokość : max. 50 mm

Wymiary z podstawą Wysokość : max. 421 mm

Szerokość : max. 553 mm

Głębokość : max. 179 mm

Zakres regulacji Tilt Wymagany, od -5 do +21 lub min. regulacja 26 stopni

Kolor obudowy czarny

Złącze 1x 15-stykowe złącze D-Sub, 1 x HDMI 1.4

Gwarancja 3 lata na miejscu u klienta

Czas reakcji serwisu - do końca następnego dnia roboczego

Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta– dokumenty potwierdzające załączyć do oferty.