Załącznik 1 do OPZ

Wymagania na dostawę i instalację Firewall -a sieciowego

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa zestawu Firewall-a sieciowego zabezpieczającego styk z Internetem do siedziby Zamawiającego, składającego się z dwóch sztuk urządzeń typu UTM spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja w miejscu styku z Internetem wskazanym przez Zamawiającego.

1. Wymagania Ogólne
   1.1. 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.
   1.2. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
   1.3. 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.
   1.4. System musi wspierać IPv4 oraz IPv6 w zakresie:
      1.4.1. Firewall.
      1.4.2. Ochrony w warstwie aplikacji.
      1.4.3. Protokołów routingu dynamicznego.
2. Redundancja, monitoring i wykrywanie awarii:
   2.1. 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.
   2.2. W ramach postępowania mają zostać dostarczone 2 urządzenia posiadające możliwość połączenia w klaster niezawodnościowy.
   2.3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
   2.4. Monitoring stanu realizowanych połączeń VPN.
   2.5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
3. Interfejsy, Dysk, Zasilanie
   3.1. System realizujący funkcję Firewall musi dysponować minimum:
      3.1.1. 18 portami 1 Gb Ethernet RJ-45.
      3.1.2. 8 portami 1 Gb Ethernet SFP.
      3.1.3. 2 portami SFP+ 10 Gb Ethernet.
   3.2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
   3.3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
   3.4. System musi być wyposażony w zasilanie AC.
4. Parametry wydajnościowe:
   4.1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 55 tys. nowych połączeń na sekundę.
   4.2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
   4.3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
   4.4. Wydajność szyfrowania IPSec VPN nie mniej niż 11 Gbps.
   4.5. 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 2.5 Gbps.

4.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
4.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

5. Funkcje Systemu Bezpieczeństwa:
5.1. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
5.1.1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
5.1.2. Kontrola Aplikacji.
5.1.3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
5.1.4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5.1.5. Ochrona przed atakami - Intrusion Prevention System.
5.1.6. Kontrola stron WWW.
5.1.7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
5.1.8. Zarządzanie pasmem (QoS, Traffic shaping).
5.1.9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
5.1.10. 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.
5.1.11. Analiza ruchu szyfrowanego protokołem SSL.
5.1.12. Analiza ruchu szyfrowanego protokołem SSH.

6. Polityki, Firewall
6.1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
6.2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
6.3. Translację jeden do jeden oraz jeden do wielu.
6.4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
6.5. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
6.6. 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.
6.6.1. Amazon Web Services (AWS).
6.6.2. Microsoft Azure
6.6.3. Cisco ACI.
6.6.4. Google Cloud Platform (GCP).
6.6.5. OpenStack.
6.6.6. VMware vCenter (ESXi).

7. Połączenia VPN
7.1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
7.1.1. Wsparcie dla IKE v1 oraz v2.
7.1.2. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
7.1.3. Obsługa protokołu Diffie-Hellman grup 19 i 20.
7.1.4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
7.1.5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
7.1.6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
7.1.7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
7.1.8. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
7.1.9. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
7.2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

7.2.1. 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.
7.2.2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
7.2.3. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

8. Routing i obsługa łączy WAN. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
8.1. Routingu statycznego.
8.2. Policy Based Routingu.
8.3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
9. Zarządzanie pasmem
9.1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
9.2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
9.3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
10. Ochrona przed malware
10.1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
10.2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
10.3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
10.4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze.
10.5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
11. Ochrona przed atakami
11.1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
11.2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
11.3. Baza sygnatur ataków powinna zawierać minimum 18000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
11.4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
11.5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
11.6. 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.
11.7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
12. Kontrola aplikacji
12.1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
12.2. Baza Kontroli Aplikacji powinna zawierać minimum 5000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
12.3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
12.4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
12.5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
13. Kontrola WWW
13.1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 260 milionów adresów URL pogrupowanych w kategorie tematyczne.
13.2. 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.
13.3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

13.4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
13.5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
13.6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
13.7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

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

15. Zarządzanie
15.1. 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.
15.2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
15.3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
15.4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
15.5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
15.6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
15.7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

16. Logowanie
16.1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji logowania i raportowania udostępnianej w chmurze, lub do komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
16.2. 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.
16.3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
16.4. Musi istnieć możliwość logowania do serwera SYSLOG.

17. Serwisy i licencje
17.1. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum 36 miesięcy od daty Protokołu Odbioru.

18. System musi być objęty serwisem gwarancyjnym producenta przez okres min. 36 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.
19. W ramach zamówienia wymagane jest także dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych,

systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń, spełniające poniższe wymagania minimalne:

19.1. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
19.2. System musi dysponować co najmniej 2 portami Gigabit Ethernet RJ-45.
19.3. Rozwiązanie musi dysponować powierzchnią dyskową min. 4 TB.
19.4. Z punktu widzenia bezpieczeństwa platformy, na których realizowane będą funkcje logowania muszą mieć możliwość rozbudowy o mechanizmy zabezpieczające przed utratą danych w przypadku awarii nośnika – minimum RAID 0, 1.
19.5. Parametry wydajnościowe:
  19.5.1. System musi być w stanie przyjmować minimum 25 GB logów na dzień.
  19.5.2. System musi być w stanie przeanalizować minimum 500 logów na sekundę.
  19.5.3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 50 systemów.
19.6. W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:
  19.6.1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
  19.6.2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
  19.6.3. Możliwość dostosowania widoku wyświetlanych logów poprzez dodawanie, usuwanie oraz zmianę kolejności kolumn zawierających elementy logowanego zdarzenia.
  19.6.4. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia NGFW oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa na przestrzeni zadanego czasu. Muszą one obejmować co najmniej:
  19.6.5. Listę najczęściej wykrywanych ataków
  19.6.6. Listę najbardziej aktywnych użytkowników/źródeł ruchu
  19.6.7. Listę najczęściej wykorzystywanych aplikacji
  19.6.8. Listę najczęściej odwiedzanych stron www
  19.6.9. Listę krajów, do których nawiązywane są połączenia
  19.6.10. Listę najczęściej wykorzystywanych polityk Firewall
  19.6.11. Informacje o realizowanych połączeniach IPSec i SSL VPN
  19.6.12. Listę najczęściej występujących zdarzeń systemowych
  19.6.13. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych za pomocą protokołu Syslog i/lub CEF. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
  19.6.14. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem portów UDP/514 oraz TCP/514.
  19.6.15. System musi umożliwiać cykliczny eksport logów do zewnętrznego systemu w celu ich długoterminowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP i/lub SCP. Administrator musi mieć możliwość określenia, kiedy ma następować eksport logów.
  19.6.16. System musi prezentować informacje na temat ilości przestrzeni dyskowej wykorzystanej na przechowywanie logów.
19.7. W zakresie raportowania system musi zapewniać:
  19.7.1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.
  19.7.2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
  19.7.3. Funkcję definiowania własnych raportów.
  19.7.4. Możliwość spolszczenia raportów.
  19.7.5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email oraz automatycznego przesłania raportu na zewnętrzny serwer za pomocą protokołu FTP lub SCP.
  19.7.6. Możliwość filtrowania danych uwzględnianych w procesie tworzenia danego raportu, m.in. możliwość ograniczenia zakresu raportu do danych z wybranych urządzeń NGFW a także z wybranej adresacji IP.
  19.7.7. Możliwość automatycznego usuwania raportów po określonym czasie.
19.8. Korelacja logów:

19.8.1. W zakresie korelacji zdarzeń system musi zapewniać:
19.8.2. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
19.8.3. Możliwość tworzenia własnych reguł korelowania logów.
19.8.4. Konfigurację powiadomień poprzez: e-mail, SNMP oraz API http w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. W treści powiadomienia musi być możliwość przekazania dodatkowych informacji o zdarzeniu wywołującym dane powiadomienie, np. nazwa wykrytego zagrożenia.
19.8.5. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System powinien korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
19.8.5.1. Malware/AV
19.8.5.2. Aplikacje sieciowe
19.8.5.3. Email
19.8.5.4. IPS
19.8.5.5. Web Filter
19.8.5.6. Traffic (logi z ruchu sieciowego)
19.8.5.7. Systemowe (m.in. utracone połączenie VPN, utracone połączenie sieciowe, zdarzenia związane z klastrem niezawodnościowym, zmiana w sieci SD-WAN)
19.8.6. Możliwość automatycznego, zwrotnego powiadomienia systemu bezpieczeństwa NGFW o wystąpieniu wybranych zdarzeń korelacji.
19.9. Zarządzanie:
19.9.1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
19.9.2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, Tacacs+, PKI.
19.9.3. System musi umożliwiać definiowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do wybranych modułów systemu logowania i raportowania.
19.9.4. System musi mieć możliwość podziału na wirtualne systemy logowania i raportowania (konteksty/domeny). Musi istnieć możliwość przypisywania administratorom praw dostępu do wybranych kontekstów. Dla każdego kontekstu musi być możliwość niezależnego przydzielania zasobów dyskowych oraz określania maksymalnego czasu przechowywania logów.
19.10. System musi być objęty serwisem gwarancyjnym producenta przez okres min. 36 miesięcy. W ramach tego serwisu producent musi zapewniać dostęp do aktualizacji oprogramowania oraz wsparcie techniczne.

Załącznik 2 do OPZ

Wymagania na dostawę i instalację aktualizacji oprogramowania UTM

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa aktualizacji oprogramowania posiadanego przez Zamawiającego urządzenia Stormshield SN310, do siedziby Zamawiającego, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja w miejscu styku z Internetem wskazanym przez Zamawiającego.
Zamawiający dopuszcza rozwiązanie równoważne polegające na dostawie i instalacji równoważnego systemu bezpieczeństwa, spełniającego poniższe wymagania:

1. Wymagania Ogólne
   1.1. System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
   1.2. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
   1.3. System umożliwia budowę 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 4 administratorów do poszczególnych instancji systemu.
   1.4. System wspiera protokoły IPv4 oraz IPv6 w zakresie:
      1.4.1. Firewall.
      1.4.2. Ochrony w warstwie aplikacji.
      1.4.3. Protokołów routingu dynamicznego.
2. Redundancja, monitoring i wykrywanie awarii
   2.1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
   2.2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
   2.3. Monitoring stanu realizowanych połączeń VPN.
   2.4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
3. Interfejsy, Dysk, Zasilanie:
   3.1. System realizujący funkcję Firewall dysponuje co najmniej 5 portami Gigabit Ethernet RJ-45.
   3.2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
   3.3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
   3.4. System jest wyposażony w zasilanie AC.
4. Parametry wydajnościowe:
   4.1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
   4.2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
   4.3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
   4.4. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.
   4.5. 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 Gbps.
   4.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
   4.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

5. Funkcje Systemu Bezpieczeństwa. W ramach systemu ochrony muszą być realizowane poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
   5.1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
   5.2. Kontrola Aplikacji.
   5.3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.
   5.4. Ochrona przed malware.
   5.5. Ochrona przed atakami - Intrusion Prevention System.
   5.6. Kontrola stron WWW.
   5.7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
   5.8. Zarządzanie pasmem (QoS, Traffic shaping).
   5.9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
   5.10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
   5.11. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
   5.12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
6. Polityki, Firewall
   6.1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
   6.2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   6.3. Translację jeden do jeden oraz jeden do wielu.
   6.4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
   6.5. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
   6.6. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
   6.7. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
   6.8. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
   6.9. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
      6.9.1. Amazon Web Services (AWS).
      6.9.2. Microsoft Azure.
      6.9.3. Cisco ACI.
      6.9.4. Google Cloud Platform (GCP).
      6.9.5. OpenStack.
      6.9.6. VMware NSX.
      6.9.7. Kubernetes.
7. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   7.1. Wsparcie dla IKE v1 oraz v2.
   7.2. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   7.3. Obsługa protokołu Diffie-Hellman grup 19, 20.
   7.4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   7.5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   7.6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   7.7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   7.8. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   7.9. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.

7.10. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
7.11. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
7.12. Mechanizm „Split tunneling" dla połączeń Client-to-Site.
7.13. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
8. Routing i obsługa łączy WAN. W zakresie routingu rozwiązanie zapewnia obsługę:
8.1. Routingu statycznego.
8.2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
8.3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
8.4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
8.5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
8.6. BFD (Bidirectional Forwarding Detection).
8.7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
9. Funkcje SD-WAN
9.1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
9.2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
10. Zarządzanie pasmem
10.1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
10.2. System daje możliwość określania pasma dla poszczególnych aplikacji.
10.3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
10.4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
11. Ochrona przed malware
11.1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
11.2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
11.3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
11.4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
11.5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
11.6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
11.7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
11.8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
11.9. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
12. Ochrona przed atakami
12.1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
12.2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
12.3. Baza sygnatur ataków zawiera minimum 18000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
12.4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
12.5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

12.6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
12.7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
12.8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
13. Kontrola aplikacji
13.1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
13.2. Baza Kontroli Aplikacji zawiera minimum 5000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
13.3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
13.4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
13.5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
13.6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
13.7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
14. Kontrola WWW
14.1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 260 milionów adresów URL pogrupowanych w kategorie tematyczne.
14.2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
14.3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
14.4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
14.5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
14.6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
14.7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
14.8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
14.9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
15. Uwierzytelnianie użytkowników w ramach sesji
15.1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
15.1.1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
15.1.2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
15.1.3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
15.2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
15.3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
15.4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
16. Zarządzanie
16.1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
16.2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
16.3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

16.4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
16.5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
16.6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
16.7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
16.8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
16.9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
17. Logowanie
17.1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
17.2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
17.3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
17.4. Możliwość włączenia logowania per reguła w polityce firewall.
17.5. System zapewnia możliwość logowania do serwera SYSLOG.
17.6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
18. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
19. Serwisy i licencje. Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum 12 miesięcy od daty zainstalowania urządzenia.
20. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne.

Załącznik 3 do OPZ

Wymagania na dostawę i instalację oprogramowania antywirusowego + XDR (UG)

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa oraz instalacja i konfiguracja oprogramowania antywirusowego wraz z funkcjonalnością XDR w Urzędzie Gminy Sieradz.
Realizacja niniejszego zadania może zostać dokonana poprzez podniesienie obecnie posiadanej i użytkowanej wersji oprogramowania Bitdefender GravityZone Business Securitydla 40 użytkowników, (aktualizacje ważne do 04.02.2026 r) do Bitdefender GravityZone Business Security z dodatkową warstwą ochrony XDR dla 60 użytkowników oraz zapewnienie opieki aktualizacyjnej przez minimum 36 miesięcy od dnia 5.02.2026 roku.

Zamawiający dopuszcza dostawę równoważnego systemu antywirusowego wraz z funkcjonalnością XDR z licencją na 60 stanowisk oraz z okresem ważności opieki aktualizacyjnej przez minimum 36 miesięcy od dnia 5.02.2026 roku. Warunki dla oprogramowania równoważnego:

1. Administracja zdalna w chmurze
   1.1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
   1.2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania
   1.3. z poziomu interfejsu WWW.
   1.4. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
   1.5. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
   1.6. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
   1.7. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
   1.8. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
   1.9. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
   1.10. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
   1.11. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
   1.12. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
   1.13. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
2. Ochrona stacji roboczych
   2.1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
   2.2. Rozwiązanie musi wspierać architekturę ARM64.
   2.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
   2.4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
   2.5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
   2.6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
   2.7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
   2.8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.

2.9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogó lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
2.10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
2.11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
2.12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
2.13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
2.14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
2.15. Rozwiązanie musi posiadać funkcję blokowani nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
2.16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
  2.16.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
  2.16.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
  2.16.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
  2.16.4. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu
  2.16.5. i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
  2.16.6. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
2.17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
2.18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
2.19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
2.20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
2.21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
2.22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
2.23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
  2.23.1. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
  2.23.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
  2.23.3. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
  2.23.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
2.24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
2.25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
2.26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

2.27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
2.28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
2.29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2.30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

3. Ochrona serwera

3.1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
3.2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
3.4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
3.5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
3.6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
3.7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
3.8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
3.9. Wymagania dla ochrony serwerów Windows:
3.9.1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
3.9.2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający n hoście (HIPS).
3.9.3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
3.9.4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
3.9.5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
3.9.6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
3.9.7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
3.9.8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
3.9.9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
3.10. Wymagania dla ochrony serwerów Linux:
3.10.1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
3.10.2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3.10.3. Rozwiązanie, do celów skanowania plików na macierzach NAS/SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
3.10.4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

4. Szyfrowanie

4.1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.

4.2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
4.3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4.4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
5. Ochrona urządzeń mobilnych opartych o system Android
5.1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
5.2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
5.3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
5.4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5.5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
5.5.1. usunięcie zawartości urządzenia,
5.5.2. przywrócenie urządzenie do ustawień fabrycznych,
5.5.3. zablokowania urządzenia,
5.5.4. uruchomienie sygnału dźwiękowego,
5.5.5. lokalizację GPS.
5.6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
5.7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
5.7.1. nazwę aplikacji,
5.7.2. nazwę pakietu,
5.7.3. kategorię sklepu Google Play,
5.7.4. uprawnienia aplikacji,
5.7.5. pochodzenie aplikacji z nieznanego źródła.
6. Sandbox w chmurze
6.1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
6.2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
6.3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
6.4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
6.5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6.6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
6.7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
6.8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
6.9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
6.10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
6.11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
6.12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
6.12.1. Czysty;
6.12.2. Podejrzany;
6.12.3. Bardzo podejrzany;
6.12.4. Szkodliwy.
6.13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
6.14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.

6.15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

7. Moduł XDR

7.1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.

7.2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.

7.3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.

7.4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

7.5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica".

7.6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.

7.7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.

7.8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.

7.9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.

7.10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.

7.11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.

7.12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.

7.13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.

7.14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.

7.15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej podzespołów zarządzanego komputera, w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe oraz wylistowanie zainstalowanego oprogramowania firm trzecich.

7.16. Konsola administracyjna musi mieć możliwość tagowania obiektów.

7.17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń PowerShell.

8. Należy dostarczyć klucz produktu oraz najnowszą wersję oprogramowania na pendrive lub przesłać link na adres e-mail wskazany przez Zamawiającego, umożliwiający pobranie oprogramowania w zakupionej wersji ze strony producenta. Preferowana wersja interfejsu oprogramowania to język polski.

8.1. Należy dostarczyć instrukcję lub link do niej w języku polskim. Instrukcja musi tłumaczyć przynajmniej: proces instalacji oprogramowania na stacjach roboczych i serwerach, proces rejestracji stacji roboczych i serwerów w konsoli centralnej, instrukcję użytkowania konsoli centralnej, proces konfiguracji i użytkowania wszystkich modułów wchodzących w skład dostarczonego oprogramowania.

Załącznik 4 do OPZ

Wymagania na dostawę i instalację Oprogramowania antywirusowego + XDR (GOPS)

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa oraz instalacja i konfiguracja oprogramowania antywirusowego wraz z funkcjonalnością XDR w Gminnym Ośrodku Pomocy Społecznej Gminy Sieradz. Realizacja niniejszego zadania może zostać dokonana poprzez podniesienie obecnie posiadanej i użytkowanej wersji oprogramowania ESET PROTECT Entry (15 stanowisk, aktualizacje ważne do 12.02.2026) do wersji ESET PROTECT Enterprise oraz zapewnienie opieki aktualizacyjnej przez minimum 36 miesięcy od dnia 13.02.2026 roku.

Zamawiający dopuszcza dostawę równoważnego systemu antywirusowego wraz z funkcjonalnością XDR z licencją na 15 stanowisk oraz z okresem ważności opieki aktualizacyjnej przez minimum 36 miesięcy od dnia 13.02.2026 roku. Warunki dla oprogramowania równoważnego:

1. Administracja zdalna w chmurze
   1.1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
   1.2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
   1.3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
   1.4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
   1.5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
   1.6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
   1.7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
   1.8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
   1.9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
   1.10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
   1.11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
   1.12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
2. Ochrona stacji roboczych
   2.1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
   2.2. Rozwiązanie musi wspierać architekturę ARM64.
   2.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
   2.4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
   2.5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
   2.6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
   2.7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
   2.8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
   2.9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.

2.10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
2.11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
2.12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
2.13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
2.14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
2.15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
2.16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
  2.16.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
  2.16.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
  2.16.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
  2.16.4. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu
  2.16.5. i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
  2.16.6. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
2.17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
2.18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
2.19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
2.20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
2.21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
2.22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
2.23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
  2.23.1. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
  2.23.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
  2.23.3. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
  2.23.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
2.24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
2.25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
2.26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
2.27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
2.28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.

2.29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2.30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

3. Ochrona serwera

3.1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
3.2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3.3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
3.4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
3.5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
3.6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
3.7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
3.8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
3.9. Wymagania dla ochrony serwerów Windows:
3.9.1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
3.9.2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3.9.3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
3.9.4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
3.9.5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
3.9.6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
3.9.7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
3.9.8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
3.9.9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
3.10. Wymagania dla ochrony serwerów Linux:
3.10.1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
3.10.2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3.10.3. Rozwiązanie, do celów skanowania plików na macierzach NAS/SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
3.10.4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

4. Szyfrowanie

4.1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
4.2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).

4.3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4.4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
5. Ochrona urządzeń mobilnych opartych o system Android
5.1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
5.2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
5.3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
5.4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5.5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
5.5.1. usunięcie zawartości urządzenia,
5.5.2. przywrócenie urządzenie do ustawień fabrycznych,
5.5.3. zablokowania urządzenia,
5.5.4. uruchomienie sygnału dźwiękowego,
5.5.5. lokalizację GPS.
5.6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
5.7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
5.7.1. nazwę aplikacji,
5.7.2. nazwę pakietu,
5.7.3. kategorię sklepu Google Play,
5.7.4. uprawnienia aplikacji,
5.7.5. pochodzenie aplikacji z nieznanego źródła.
6. Sandbox w chmurze
6.1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
6.2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
6.3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
6.4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
6.5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6.6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
6.7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
6.8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
6.9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
6.10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
6.11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
6.12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
6.12.1. Czysty;
6.12.2. Podejrzany;
6.12.3. Bardzo podejrzany;
6.12.4. Szkodliwy.
6.13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
6.14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
6.15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

7. Moduł XDR
   7.1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
   7.2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
   7.3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
   7.4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
   7.5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica".
   7.6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
   7.7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
   7.8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
   7.9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
   7.10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
   7.11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
   7.12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
   7.13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
   7.14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
   7.15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej podzespołów zarządzanego komputera, w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
   7.16. Konsola administracyjna musi mieć możliwość tagowania obiektów.
   7.17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń PowerShell.
8. Należy dostarczyć klucz produktu oraz najnowszą wersję oprogramowania na pendrive lub przesłać link na wskazany adres e-mail przez Zamawiającego, umożliwiający pobranie oprogramowania w zakupionej wersji ze strony producenta. Wersja interfejsu oprogramowania to język polski.
9. Należy dostarczyć instrukcję lub link do niej w języku polskim. Instrukcja musi tłumaczyć przynajmniej: proces instalacji oprogramowania na stacjach roboczych i serwerach, proces rejestracji stacji roboczych i serwerów w konsoli centralnej, instrukcję użytkowania konsoli centralnej, proces konfiguracji i użytkowania wszystkich modułów wchodzących w skład dostarczonego oprogramowania.

Załącznik 5 do OPZ

Wymagania na rozbudowę Oprogramowania do zarządzania stanowiskami

Do obowiązków Wykonawcy w ramach niniejszego zadania należy przedłużenie opieki aktualizacyjnej posiadanego oprogramowania Axence nVision dla modułów: Inventory, Users HelpDesk, DataGuard (liczba stanowisk: 25, ważnej do 01.07.2025 r) o minimum 36 miesięcy liczonych od dnia 2.07.2025 roku wraz z rozszerzeniem liczby stanowisk do łącznie 60 sztuk.
Zamawiający dopuszcza dostawę równoważnego Oprogramowania do zarządzania stanowiskami z licencją na 60 stanowisk oraz z okresem ważności opieki aktualizacyjnej przez 36 miesięcy liczonych od dnia 2.07.2025 roku.

Warunki techniczne i funkcjonalne dla oprogramowania równoważnego:

1. Monitorowanie infrastruktury
1.1. obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:
1.1.1. wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
1.1.2. wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z OU)
1.1.3. wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
1.1.4. wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki
1.1.5. wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
1.1.6. wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
1.1.7. wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach w dowolnym rozmiarze i kolorze
1.1.8. wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
1.1.9. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
1.1.10. zablokowania mapy urządzeń przed przypadkową edycją
1.1.11. serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
1.1.12. serwerów pocztowych:
1.2. program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty
1.3. program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem)
1.4. program ma możliwość wykonywania operacji testowych
1.5. program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa w zakresie:
1.5.1. monitorowania serwerów WWW i adresów URL
1.5.2. cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
1.5.3. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail
1.5.4. obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID
1.5.5. obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
1.5.6. monitoringu routerów i przełączników wg:
1.5.6.1. zmian stanu interfejsów sieciowych
1.5.6.2. ruchu sieciowego
1.5.6.3. podłączonych stacji roboczych – graficzna prezentacja panelu switcha
1.5.6.4. ruchu generowanego przez podłączone do portów stacje robocze
1.6. serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie

1.7. wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
1.8. monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano
1.9. zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny
1.10. wydajności systemów Windows: obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

2. Inwentaryzacja
2.1. Gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych oraz:
2.1.1. Prezentacja szczegółów dotyczących sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
2.1.2. Możliwość odczytu parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
2.1.3. Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
2.1.4. Informacje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
2.1.5. Informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
2.1.6. Możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
2.1.7. Odczytanie numeru seryjnego (klucze licencyjne).
2.1.8. Automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
2.1.9. Możliwość przeglądu informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
2.1.10. Możliwość utworzenia listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI), znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
2.1.11. Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.
2.2. Możliwość prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:
2.2.1. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
2.2.2. przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,
2.2.3. tworzenia powiązań między zasobami a urządzeniami,
2.2.4. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
2.2.5. tworzenia relacji pomiędzy zasobami,
2.2.6. wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
2.2.7. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości:
2.3. dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
2.3.1. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
2.3.2. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
2.3.3. masową edycję atrybutów zasobów,
2.3.4. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
2.3.5. importu danych z zewnętrznego źródła (.CSV),
2.3.6. przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury
2.3.7. zakupu, gwarancji, dowolnego dokumentu itp.,
2.3.8. tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
2.3.9. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
2.3.10. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie,

2.3.11. konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
2.3.12. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
2.3.13. przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
2.3.14. konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
2.3.15. konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
2.3.16. archiwizacji i porównywania audytów zasobów,
2.3.17. tworzenia kodów kreskowych dla zasobów,
2.3.18. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
2.3.19. inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów,
2.3.20. dodawanie czynności serwisowych, drukowanie etykiet,
2.3.21. możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
2.3.22. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
2.3.23. definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data" z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja").

2.4. Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
2.4.1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
2.4.2. Informacje o aplikacjach używanych w organizacji.
2.4.3. Tworzenie własnych wzorców aplikacji.
2.4.4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
2.4.5. Informacje o komputerach, na których aplikacja została wykryta.
2.4.6. Zarządzanie posiadanymi licencjami.
2.4.7. Wskazywanie osób odpowiedzialnych za licencję.
2.4.8. Wskazanie użytkowników licencji.
2.4.9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
2.4.10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
2.4.11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
2.4.12. Zarządzanie posiadanymi licencjami: raport zgodności licencji.
2.4.13. Możliwość przypisania do programów numerów seryjnych, wartości.

3. Obsługa użytkowników - możliwość sprawdzenie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:
3.1. Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
3.2. Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
3.3. Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
3.4. Informacji o edytowanych przez użytkownika dokumentach,
3.5. Historii pracy (cykliczne zrzuty ekranowe),
3.6. Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),
3.7. Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),

3.8. Wydruków, w tym m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek.
3.9. Kosztów wydruków,
3.10. Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.
3.11. Wykrywanie podejrzanej aktywności przez popularne „jigglery", mającej na celu symulowanie faktycznej pracy.
3.12. Zdefiniowanie czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.
3.13. Wyszczególnienie podejrzanej aktywności w raportach.
3.14. Wygenerowanie alarmu i wykonania akcji po wykryciu podejrzanej aktywności.
3.15. Automatyczne włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności.
Blokowanie stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami.
3.16. integrację list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.
3.17. skorzystanie z wbudowanej listy stron sklasyfikowanych jako zagrożenia.
3.18. automatyczne odświeżania list stron zintegrowanych z adresów zewnętrznych.
3.19. blokowanie ruchu na wskazanych portach TCP/IP,
3.20. blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
3.21. prowadzenie rejestru naruszeń blokad,
3.22. wysyłanie powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
3.23. przygotowanie zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
3.24. definiowanie godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

4. Zdalna pomoc użytkownikom:

4.1. możliwość podglądu pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu umożliwia równoczesne podłączenie do tego samego komputera kilku administratorom.
4.2. możliwość użycia wewnętrznego komunikatora (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów).
4.3. funkcjonowanie bazy wiedzy, pomagającej użytkownikom samodzielnie rozwiązywać
4.4. najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program umożliwia informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik ma możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator ma możliwość tworzenia szkiców i archiwizowania komunikatów. Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany jest przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.
4.5. możliwość uzyskania dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.

5. Ochrona danych przed wyciekiem.

5.1. Blokowanie urządzeń i nośników danych. Możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
5.2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
5.3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
5.4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
5.5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
5.6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
5.7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
5.8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
5.9. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.
5.10. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
5.11. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
5.12. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.
6. Zarządzanie prawami dostępu do urządzeń:
6.1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
6.2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.
6.3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
6.4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
6.5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.
7. Audyt operacji na plikach na urządzeniach przenośnych:
7.1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
7.2. Podłączenie/odłączenie urządzenia przenośnego.
8. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. Definiowanie reguł monitorowanych folderów w postaci list.
9. Ochrona przed usunięciem. Program musi być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.
10. Instalator programu musi być zabezpieczony podpisem cyfrowym wystawionym i zweryfikowanym przez zaufany globalny urząd certyfikacji (CA).
11. Program musi być dostępny w języku polskim
12. Do programu musi być dostępny podręcznik użytkownika w języku polskim w formie papierowej lub w formie elektronicznej dostępnej poprzez stronę internetową.
13. Wsparcie techniczne musi być świadczone telefonicznie lub mailowo w języku polskim lub angielskim.

Załącznik 6 do OPZ

Wymagania na dostawę i instalację Serwera Backupu

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa Serwera Backupu do siedziby Zamawiającego, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja.

1. Obudowa
   1.1. Typu Rack o wysokości 2U
   1.2. 12 wnęk na dyski 3.5”
   1.3. Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej
   1.4. 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.
2. Płyta główna
   2.1. Płyta główna z możliwością zainstalowania do dwóch procesorów.
   2.2. Obsługa procesorów 32 rdzeniowych.
   2.3. Płyta główna zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
   2.4. Na płycie głównej powinno znajdować się 16 slotów przeznaczonych do instalacji pamięci.
   2.5. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
3. Chipset: dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
4. Procesory: zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 169 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
5. Pamięć RAM: 64GB DDR5 RDIMM 5600MT/s,
6. Kontroler RAID - sprzętowy kontroler dyskowy, posiadający
   6.1. Min. 8GB nieulotnej pamięci cache,
   6.2. Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
   6.3. Wsparcie dla dysków samoszyfrujących
7. Zainstalowane dyski twarde
   7.1. 8x dysk SAS o pojemności min. 4TB, Hot-Plug
   7.2. dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
8. Gniazda PCI: Cztery sloty PCIe
9. Interfejsy sieciowe/FC/SAS
   9.1. Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
   9.2. Dwuportowa karta sieciowa 10Gb Ethernet w standardzie BaseT
   9.3. Dwie czteroportowe karty 12Gb SAS HBA
10. Wbudowane porty
    10.1. 4 porty USB w tym min:
    10.2. 1 port USB 3.0 z tyłu obudowy,
    10.3. 1 port micro USB z przodu obudowy
    10.4. 2 port VGA z czego jeden z przodu obudowy
    10.5. Możliwość rozbudowy o port RS232
11. Video: Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
12. Wentylatory: Redundantne, Hot-Plug
13. Zasilacze: Redundantne, Hot-Plug min. 1100W klasy Titanium
14. Elementy montażowe:
    14.1. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych

14.2. Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
15. System operacyjny: Microsoft Windows Server 2025 Standard w ilości core zgodnej z zaoferowanymi procesorami w serwerze.
16. Bezpieczeństwo
    16.1. Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
    16.2. Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania.
    16.3. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
    16.4. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
    16.5. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
    16.6. Moduł TPM 2.0
    16.7. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie, bez potrzeby restartu serwera
    16.8. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
    16.9. Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
17. Karta zarządzania: niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:
    17.1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
    17.2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
    17.3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
    17.4. możliwość podmontowania zdalnych wirtualnych napędów;
    17.5. wirtualną konsolę z dostępem do myszy, klawiatury;
    17.6. wsparcie dla IPv6;
    17.7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
    17.8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
    17.9. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
    17.10. integracja z Active Directory;
    17.11. możliwość obsługi przez dwóch administratorów jednocześnie;
    17.12. wsparcie dla automatycznej rejestracji DNS
    17.13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
    17.14. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
    17.15. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o:
        17.15.1. Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej
        17.15.2. Przesyłanie danych telemetrycznych w czasie rzeczywistym
        17.15.3. Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze
        17.15.4. Automatyczna rejestracja certyfikatów (ACE)
18. Biblioteka taśmowa
    18.1. Wysokość maksymalnie 1U do instalacji w szafie Rack.
    18.2. 9 slotów przeznaczonych na zestaw taśm.
    18.3. Port SAS o przepustowości co 6Gb/s w standardzie umożliwiającym podłączenie serwerów.
    18.4. Napęd wyposażony w co najmniej 1 sztukę napędu SAS LTO 8.
    18.5. kabel SAS umożliwiający podłączenie biblioteki do serwera o dł. min. 2m
    18.6. 10 x taśma LTO8
    18.7. 1 x taśma czyszcząca

19. Oprogramowanie do zarządzania: możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:
    19.1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
    19.2. Integracja z Active Directory
    19.3. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
    19.4. Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
    19.5. Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
    19.6. Szczegółowy opis wykrytych systemów oraz ich komponentów
    19.7. Możliwość eksportu raportu do CSV, HTML, XLS, PDF
    19.8. Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
    19.9. Grupowanie urządzeń w oparciu o kryteria użytkownika
    19.10. Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
    19.11. Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
    19.12. Szybki podgląd stanu środowiska
    19.13. Podsumowanie stanu dla każdego urządzenia
    19.14. Szczegółowy status urządzenia/elementu/komponentu
    19.15. Generowanie alertów przy zmianie stanu urządzenia.
    19.16. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
    19.17. Integracja z service desk producenta dostarczonej platformy sprzętowej
    19.18. Możliwość przejęcia zdalnego pulpitu
    19.19. Możliwość podmontowania wirtualnego napędu
    19.20. Kreator umożliwiający dostosowanie akcji dla wybranych alertów
    19.21. Możliwość importu plików MIB
    19.22. Przesyłanie alertów „as-is” do innych konsol firm trzecich
    19.23. Możliwość definiowania ról administratorów
    19.24. Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
    19.25. Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta rozwiązania)
    19.26. Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
    19.27. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
    19.28. 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.
    19.29. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
    19.30. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
    19.31. Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
    19.32. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
    19.33. Zdalne uruchamianie diagnostyki serwera.
    19.34. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
    19.35. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
20. Oprogramowanie do monitorowania: oparta na chmurze aplikacja producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Rozwiązanie musi posiadać następujące funkcjonalności:
    20.1. Monitoring:
        20.1.1. ilość podłączonych oraz rozłączonych systemów
        20.1.2. stan podłączonych urządzeń
        20.1.3. informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów
        20.1.4. informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia
        20.1.5. informacje o statusie gwarancji dla poszczególnych urządzeń

20.1.6. informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń
20.1.7. informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.
20.1.8. Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych
20.1.9. Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych.
20.1.10. Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.
20.1.11. Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.
20.1.12. Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.
20.1.13. Monitoring parametrów serwerów z informacją o minimum:
20.1.13.1. Obciążeniu procesora
20.1.13.2. Zużyciu pamięci RAM
20.1.13.3. Temperaturze procesorów
20.1.13.4. Temperaturze powietrza wlotowego
20.1.13.5. Zużyciu prądu
20.1.13.6. Zmianach w fizycznej konfiguracji serwera
20.1.13.7. Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
20.1.14. Monitoring parametrów pamięci masowych z informacją o minimum:
20.1.14.1. Opóźnieniach
20.1.14.2. IOPS
20.1.14.3. Przepustowości
20.1.14.4. Utylizacji kontrolerów
20.1.14.5. Pojemność całkowita i dostępna
20.1.14.6. Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.
20.1.14.7. Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
20.1.14.8. Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
20.1.14.9. Informacje o poziomie redukcji danych
20.1.14.10. Informacje o statusie replikacji oraz snapshotów
20.1.15. Monitoring parametrów przełączników sieciowych z informacją o minimum:
20.1.15.1. Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
20.1.15.2. Stanie komponentów: zasilacze, wentylatory
20.1.15.3. Podłączonych hostach
20.1.15.4. Ilości i statusu portów
20.1.15.5. Utylizacji procesora
20.1.15.6. Utylizacji poszczególnych portów
20.1.15.7. Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
20.1.16. Aktualizacja firmware:
20.1.16.1. oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
20.1.16.2. oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
20.1.16.3. oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania
20.1.16.4. dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
20.1.16.5. dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania

20.2. Raporty
20.2.1. Możliwość generowania raportów dla serwerów zawierających informację o nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym

systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej, średnim obciążeniu: procesorów, pamięci RAM, IO,

20.2.2. Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji

20.2.3. Generowanie raportów do plików CSV i PDF

20.3. Cyberbezpieczeństwo

20.3.1. Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.

20.3.2. Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.

20.3.3. Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.

20.3.4. Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.

20.4. Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;

20.5. Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.

20.6. Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android

21. Certyfikaty

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

21.2. Serwer musi posiadać deklarację CE.

21.3. 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 Silver według normy wprowadzonej w 2019 roku - Dokumenty potwierdzające Wykonawca dostarczy na etapie dostawy w terminie 14 dni kalendarzowych od dnia podpisania umowy, jednak nie później niż 1 dzień roboczy przed rozpoczęciem fizycznych dostaw sprzętu komputerowego.

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

22. Dokumentacja użytkownika

22.1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

22.2. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

23. Warunki gwarancji. Zamawiający wymaga zapewnienia

23.1. gwarancji producenta serwera na okres 36 miesięcy.

23.2. możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365, telefonicznie i przez Internet.

23.3. pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także oprogramowania.

23.4. możliwości samodzielnego kwalifikowania poziomu ważności naprawy.

23.5. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.

23.6. Naprawa ma się odbyć w siedzibie Zamawiającego, chyba, że Zamawiający dla danej naprawy zgodzi się na inną formę nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę

i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.

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

23.8. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:

23.9. Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie Zamawiającego.

23.10. Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.

23.11. Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.

23.12. Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.

23.13. Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.

23.14. Wymagane oświadczenie Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. - Dokumenty potwierdzające Wykonawca dostarczy na etapie dostawy w terminie 14 dni kalendarzowych od dnia podpisania umowy, jednak nie później niż 1 dzień roboczy przed rozpoczęciem fizycznych dostaw sprzętu komputerowego.

23.15. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. - Dokumenty potwierdzające Wykonawca dostarczy na etapie dostawy w terminie 14 dni kalendarzowych od dnia podpisania umowy, jednak nie później niż 1 dzień roboczy przed rozpoczęciem fizycznych dostaw sprzętu komputerowego.

Załącznik 7 do OPZ

Wymagania na dostawę i instalację Network Attached Storage

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa 2 sztuk urządzeń typu Network Attached Storage do siedziby Zamawiającego, spełniających minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja.

I. Network Attached Storage – typ A

1. Typ obudowy przystosowana do montażu w szafie rack 19”, max. 2U z możliwością instalacji min. 24 dysków 2.5”
2. Zainstalowane:7 x dysk SSD SAS o pojemności min. 1.6TB, Hot-Plug
3. Możliwość rozbudowy (bez wymiany kontrolerów), do co najmniej 276 dysków twardych.
4. Możliwość obsługiwania dysków SSD, SAS i Nearline SAS.
5. Możliwość mieszania napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej.
6. Obsługa dysków 2,5” oraz 3,5”.
7. Obsługa mechanizmu RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji i z wykorzystaniem wszystkich dysków (tzw. wide-striping).
8. Możliwość definiowania globalnych dysków spare oraz dedykowanie dysków spare do grup RAID.
9. Możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności, zwiększenie szybkości odbudowy na wypadek awarii dysku).
10. Obsługa dysków różnej pojemności w ramach grupy dysków.
11. Tryb pracy kontrolerów - minimum 2 kontrolery pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
12. Pamięć cache minimum sumarycznie 32 GB pamięci cache w oparciu o wydajną pamięć typu RAM.
13. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.
14. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
15. Rozbudowa pamięci cache musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
16. Interfejsy: co najmniej 8 portów 12Gb SAS (4 porty na kontroler)
17. Kable/wkładki: 4x kabel 12Gb HD Mini-SAS/HD Mini-SAS min. 2m
18. Zarządzanie musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie musi odbywać się bezpośrednio na kontrolerach z poziomu przeglądarki internetowej.
19. Zarządzanie grupami dyskowymi oraz dyskami logicznymi: musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych.
20. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.
21. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
22. Thin Provisioning - musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.
23. Możliwość odzyskiwania przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
24. Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.
25. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.

26. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
27. Wewnętrzne kopie migawkowe - dokonywanie na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time za pomocą wewnętrznych kontrolerów. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.
28. Minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
29. Wewnętrzne kopie pełne - dokonywanie na żądanie pełnej fizycznej kopii danych (clone) za pomocą wewnętrznych kontrolerów. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
30. Migracja danych musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
31. Podłączanie zewnętrznych systemów operacyjnych - jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).
32. Wsparcie podłączenia systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.
33. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
34. Redundancja- urządzenie nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.
35. Możliwość wymiany elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.
36. Możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
37. Zasilacze powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.
38. Oferowany system dyskowy musi się składać z pojedynczego urządzenia. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu urządzeń. Za pojedyncze urządzenia nie uznaje się rozwiązania opartego o dwa lub więcej urzadzeń dyskowych (par kontrolerów) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem urządzeń dyskowych.
39. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
40. Urządzenie musi spełniać następujące standardy bezpieczeństwa:
    40.1. EN 62368-1 (European Union),
    40.2. IEC 60950-1 (International)
41. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami:
    41.1. ISO 9001
    41.2. ISO 14001
42. Deklaracja zgodności CE
43. Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego urządzenia, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.
44. Warunki gwarancji
    44.1. Zamawiający wymaga zapewnienia gwarancji Producenta na okres min. 36 miesięcy.
    44.2. Zamawiający wymaga możliwości odpłatnego przedłużenia gwarancji Producenta na okres min. 7 lat.

44.3. Zamawiający wymaga możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie (infolinia prowadzona w języku polskim) i przez Internet.
44.4. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
44.5. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
44.6. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.
44.7. Naprawa ma się odbyć w siedzibie Zamawiającego, chyba, że Zamawiający dla danej naprawy zgodzi się na inną formę.
44.8. Zamawiający wymaga nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
44.9. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia na etapie dostawy oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Dokumenty potwierdzające Wykonawca dostarczy na etapie dostawy w terminie 14 dni kalendarzowych od dnia podpisania umowy, jednak nie później niż 1 dzień roboczy przed rozpoczęciem fizycznych dostaw sprzętu komputerowego.
44.10. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii.
44.11. Charakterystyka usługi diagnostyki:
  44.11.1. Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie Zamawiającego.
  44.11.2. Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
  44.11.3. Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.
  44.11.4. Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.
  44.11.5. Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.
44.12. Wymagane oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
44.13. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.

II. Network Attached Storage – typ B

1. Wymagania ogólne:
   1.1. Procesor: zainstalowany min. jeden dwurdzeniowy klasy x86 – 64 bity, umożliwiający osiągnięcie wyniku min. 3200 punktów w teście Passmark CPU, dostępnym na stronie www.cpubenchmark.net. Do oferty należy załączyć wydruk ze strony potwierdzający osiągnięty wynik od momentu zamieszczenia ogłoszenia o przetargu do terminu składania ofert.
   1.2. Częstotliwość procesora 2.6 (podstawowy) / 3.1 (turbo) GHz
   1.3. Mechanizm szyfrowania sprzętowego
2. Pamięć
   2.1. Pamięć systemowa 8 GB DDR4 ECC SODIMM
   2.2. Fabrycznie zainstalowany moduł pamięci 8 GB
   2.3. Całkowita liczba gniazd pamięci: 2
   2.4. Maksymalna pojemność pamięci: 32 GB (16 GB x 2)
3. Pamięć masowa
   3.1. Zatoki dyskowe SATA: min. 5
   3.2. Zatoki dyskowe M.2: min. 2 (NVMe)
   3.3. Zgodny typ dysków: 3.5" SATA HDD, SATA SSD 2,5”, M.2 2280 NVMe SSD
   3.4. Dysk HDD i SSD z możliwością wymiany podczas pracy (hot-swap)
4. Wyposażenie w dyski – 4 sztuki o parametrach:
   4.1. 3,5-calowe dyski SATA HDD o pojemności 4 TB każdy
   4.2. Prędkość obrotowa: 5400 obr/min
   4.3. Interfejs dysku: SATA III – 6 Gb/s
5. Porty zewnętrzne
   5.1. Port LAN RJ45 1GbE: min. 4
   5.2. Port USB 3.2 1. Generacji: 2
   5.3. Gniazdo rozszerzenia: 2
   5.4. Typ portu rozszerzeń: eSATA
   5.5. PCIe - Rozszerzenie karty PCIe: 1 x Gen3 x 2 Gniazdo aktualizacji sieci
6. Ogólne
   6.1. Przywracanie zasilania: tak
   6.2. Natężenie dźwięku* max 22 dBA
   6.3. Zaplanowane włączanie/wyłączanie: tak
   6.4. Zasilacz / Adapter: 120 watów
7. Zarządzanie przechowywaniem
   7.1. Maksymalny rozmiar pojedynczego wolumenu: 108 TB
   7.2. Maks. liczba wolumenów wewnętrznych: 64
   7.3. Obsługa puli pamięci M.2 SSD
   7.4. SSD TRIM
8. Obsługiwane typy macierzy RAID:
   8.1. Basic
   8.2. JBOD
   8.3. RAID 0
   8.4. RAID 1
   8.5. RAID 5
   8.6. RAID 6
   8.7. RAID 10
9. Obsługiwane wewnętrzne dyski twarde:
   9.1. Btrfs
   9.2. ext4
10. Obsługiwane zewnętrzne dyski twarde:
   10.1. Btrfs
   10.2. ext4
   10.3. ext3
   10.4. FAT
   10.5. NTFS
   10.6. HFS
   10.7. exFAT

11. Obsługiwane protokoły plików:
    11.1. SMB
    11.2. AFP
    11.3. NFS
    11.4. FTP
    11.5. WebDAV
    11.6. Rsync
    11.7. Maks. liczba jednoczesnych połączeń protokołu SMB/AFP/FTP: 2,000
    11.8. Maks. liczba jednoczesnych połączeń protokołu SMB/AFP/FTP (z rozbudową pamięci RAM): 2.000
    11.9. Integracja listy kontroli dostępu systemu Windows ACL: tak
    11.10. Uwierzytelnienie NFS Kerberos: tak
12. Konto i folder współdzielony
    12.1. Maksymalna liczba lokalnych kont użytkowników: 2,048
    12.2. Maksymalna liczba lokalnych grup: 256
    12.3. Maks. liczba folderów udostępnionych: 512
    12.4. Maks. liczba zadań synchr. folderów udostępnionych: 32
13. Kopie zapasowe folderów i pakietów : tak
14. Kopia zapasowa całego systemu: tak
15. Centrum logów – wymagana liczba zdarzeń Syslog na sekundę: 800
16. Wirtualizacja:
    16.1. VMware ESXi 6.5 and VAAI
    16.2. Windows Server 2022
    16.3. Citrix Ready
    16.4. OpenStack
17. Obsługiwane protokoły:
    17.1. SMB1 CIFS, SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS, Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP,LDAP, CalDAV
18. Obsługiwane przeglądarki:
    18.1. Chrome
    18.2. Firefox
    18.3. Edge
    18.4. Safari
19. Deklaracja CE
20. Obsługiwane języki: Polski
21. Gwarancja na sprzęt – 36 miesięcy.

Załącznik 8 do OPZ

Wymagania na dostawę i instalację Oprogramowania kopii zapasowych

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa i instalacja Oprogramowania kopii zapasowych w siedzibie Zamawiającego, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej.

1. Wymagania ogólne
   1.1. Dostarczone oprogramowanie musi umożliwiać wykonywanie kopii zapasowych z minimum 20 maszyn wirtualnych pracujących w środowisku wirtualizacyjnym (składającym się z 3 serwerów wirtualizacyjnych) lub 20 serwerów fizycznych, każdy z własną instancją systemu operacyjnego.
   1.2. Oprogramowanie musi być objęte wsparciem technicznym producenta przez okres 36 miesięcy.
   1.3. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5.
   1.4. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
   1.5. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
2. Wymagania funkcjonalne, oprogramowanie musi
   2.1. być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
   2.2. tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
   2.3. mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
   2.4. 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.
   2.5. 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.
   2.6. pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
   2.7. wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
   2.8. nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
   2.9. oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
   2.10. zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
   2.11. mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
   2.12. mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
   2.13. mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności.
   2.14. posiadać mechanizmy chroniące przed utratą hasła szyfrowania

2.15. posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
2.16. posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
2.17. wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora)
2.18. posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)
2.19. posiadać integracje z systemami typu SIEM
2.20. posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej.

3. Wymagania RPO - oprogramowanie musi;
3.1. wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
3.2. wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
3.3. 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 z dokładnością do pojedynczego datastoru
3.4. zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów oraz zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Wykonanie kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Funkcjonalność musi działać w środowisku VMware.
3.5. posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
3.6. wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).
3.7. mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
3.8. wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
3.9. 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.
3.10. mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
3.11. 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.
3.12. 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 punku w ramach ustalonego parametru RPO.
3.13. umożliwiać przechowywanie punktów przywracania dla replik
3.14. umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
3.15. wykorzystywać wszystkie tryby transportu hypervisora (sieć, hot-add, LAN Free-SAN)

4. Wymagania RTO - oprogramowanie musi:
4.1. 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.
4.2. dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
4.3. 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
4.4. pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre

4.5. pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
4.6. umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
4.7. umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
4.8. umożliwić odtworzenie plików/folderów lub ich uprawnień 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
4.9. mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
4.10. wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
4.11. wspierać przywracanie plików z partycji Linux LVM
4.12. umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
4.13. wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
4.14. wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
4.15. wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
4.16. wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
4.17. wspierać granularne odtwarzanie baz Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność musi być dostępna dla baz uruchomionych w Windows oraz Linux.
4.18. wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
4.19. wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji
4.20. posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
4.21. posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
4.22. posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
4.23. posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2
4.24. wspierać metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

5. Ograniczenie ryzyka, oprogramowanie musi:

5.1. dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu, funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
5.2. dla VMware'a pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
5.3. 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
5.4. 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.
5.5. analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware
5.6. mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania
5.7. bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków

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

6. Środowiska fizyczne musi:

6.1. wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
6.2. wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
6.3. wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
6.4. wspierać system operacyjny macOS
6.5. wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
6.6. mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
6.7. wspierać systemy oparte o Microsoft Failover Cluster
6.8. wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
6.9. wspierać backup podłączonych dysków USB
6.10. kopia zapasowa maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
6.11. pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
6.12. wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
6.13. wspierać kontrolę pasma sieciowego
6.14. wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
6.15. wspierać ograniczenia wykonywania backupów dla połączeń VPN
6.16. wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft.
6.17. wspierać technologię BitLocker
6.18. wspierać uruchamianie z nośnika odtwarzania
6.19. wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
6.20. wspierać odzysk do punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
6.21. umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
6.22. wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
6.23. wspierać szyfrowanie
6.24. wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
6.25. posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
6.26. posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
6.27. wspierać tworzenie wielu zadań backupowych

7. Monitoring, system musi:

7.1. zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
7.2. umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
7.3. umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 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.

7.4. umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii w vCenter
7.5. umożliwiać tworzenie alarmów dla grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
7.6. dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
7.7. dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
7.8. mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
7.9. mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
7.10. mieć konsolę z sumarycznym podglądem obiektów infrastruktury wirtualnej (ang. Dashboard)
7.11. mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
7.12. zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
7.13. mieć możliwość integracji z oprogramowaniem do kopii zapasowych tego samego producenta
7.14. mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji i weryfikacji odzyskiwalności maszyn wirtualnych.
7.15. 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.
7.16. mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
7.17. mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4

8. Raportowanie, system musi:
8.1. umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 w bezpłatnej wersji ESXi, w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter lub pracujące samodzielnie
8.2. umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 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.
8.3. wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
8.4. być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
8.5. mieć możliwość eksportowania raportów do formatów Microsoft Word, Excel, Visio, Adobe PDF
8.6. mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
8.7. mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
8.8. mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
8.9. mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
8.10. posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
8.11. mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
8.12. mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
8.13. mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
8.14. mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.
8.15. mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
8.16. mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
8.17. mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.

Załącznik 9 do OPZ

Wymagania na dostawę i instalację UPS 3kVA z bateriami

Do obowiązków Wykonawcy w ramach niniejszego zadania należy dostawa UPS 3kVA z bateriami do siedziby Zamawiającego, spełniającego minimalne wymagania techniczne i funkcjonalne określone poniżej oraz jego instalacja i konfiguracja. Wymagania minimalne:

1. Technologia: online, VFI-SS-111,
2. Moc wyjściowa: 3kVA/3kW; PF=1
3. Obudowa: typu rack lub tower z zestawem do montażu w szafie rack na wyposażeniu
4. Napięcie wejściowe: 110 ÷ 300 V AC ± 2 %
5. Napięcie znamionowe (wartość skuteczna): 230V AC
6. Prąd znamionowy (wejście) 15,6A
7. Częstotliwość napięcia wejściowego (zakres oraz tolerancja): 45 ÷ 55 / 55 ÷ 65 Hz ± 1 Hz
8. Częstotliwość znamionowa napięcia wejściowego 50Hz / 60Hz
9. Zniekształcenia prądu wejściowego THDi < 5%
10. Zakres napięcia wyjściowego: 200/208/220/230/240V AC konfigurowalne z poziomu oprogramowania oraz z menu zasilacza na wyświetlaczu LCD (domyślnie 230V AC
11. Zniekształcenia napięcia wyj. THDu < 1% dla Pmax (liniowe); < 5% (nieliniowe PN EN 62040-3
12. Gniazda wyjściowe 4x IEC320 C13 (10A) sterowalne + 4x IEC320 C13 (10A) + 1x IEC320 C19 (16A)
13. Akumulatory wewnętrzne UPS: minimum 6szt akumulatorów 12V 9Ah
14. Możliwość podpięcia do 4szt modułów bateryjnych (każdy z minimum 12szt akumulatorów 12V9Ah)
15. Czas podtrzymania UPS dla obciążenia 3kW/2,5kW/1,5kW 3 / 4 / 9 min
16. Czas podtrzymania UPS i dołączonego modułu dla obciążenia 3kW/2,5kW/1,5kW min: 16 / 21 / 39 min
17. Przeciążalność: 105-125% - 5min / 125-150% - 30s / >150% - 500ms
18. EPO wg standardu NC
19. Sygnalizacja akustyczno-diodowa, wyświetlacz LCD oraz diody sygnalizujące usterkę, pracę bateryjną, pracę w trybie online, obejście bypass
20. Język oprogramowania: polski i angielski do wyboru z poziomu interfejsu użytkownika
21. Konfiguracja minimalnego poziomu naładowania baterii po powrocie zasilania sieciowego (po rozładowaniu baterii przed ponownym samoczynnym załączeniem zasilania na wyjściu) Wymagane, konfigurowalne z poziomu oprogramowania (przez USB)
22. Certyfikaty: CE oraz ISO 9001:2015 dla producenta sprzętu na proces projektowania, produkcji i serwisu;
23. Komunikacja z urządzeniem: RS232, USB HID, styki bezpotencjałowe 1-wejście; 1-wyjście; SNMP – karta dołączona do zestawu
24. Wymiary UPS (rack) (wys x szer x gł)- nie więcej niż 86 x 439 x 600 mm
25. Oprogramowanie do monitorowania pracy zasilacza UPS - bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na min. 75 stanowiskach komputerowych w sieci; pod Windows 10, 11, Windows Server 2019, 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów
26. Oprogramowanie - funkcjonalność możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPS'ów w oprogramowaniu
27. Oprogramowanie - funkcjonalność Konfiguracja minimalnego poziomu naładowania baterii. UPS po rozładowaniu baterii przed samoczynnym załączeniem zasilania wyjść (po powrocie zasilania sieciowego) będzie musiał naładować baterie do tego poziomu. Parametr ten ma zastosowanie w przypadku, gdy załączenie zasilania wyjść może nastąpić tylko wtedy, gdy UPS zgromadzi niezbędny zapasa energii na wypadek kolejnego zaniku.
28. Oprogramowanie - funkcjonalność Uruchom poprzez Bypass - Aktywacja tej funkcji powoduje, że UPS zawsze przed załączeniem zasilania wyjść na kilka sekund załączy zasilanie poprzez Bypass i po chwili przełączy się w zasilanie wyjść poprzez falownik (normalny tryb pracy).
29. Serwis producenta, autoryzacja serwisowa lub oświadczenie producenta o prowadzeniu serwisu.
30. Gwarancja: minimum 36 miesięcy na elektronikę i akumulatory,
31. Serwis door to door, czas naprawy do 5 dni roboczych
32. Dokumentacja w języku polskim.

Załącznik 10 do OPZ

Wymagania na usługi instalacji i konfiguracji

Do obowiązków Wykonawcy w ramach niniejszego zadania należy wykonanie usług instalacji i konfiguracji o minimalnym zakresie określonym poniżej.

1. Opracowania projektu technicznego dla całego przedsięwzięcia oraz zakresu wdrożenia zakończone akceptacją Zamawiającego.
2. Zaktualizowania oprogramowania/sterowników/firmware dla wszystkich wdrażanych rozwiązań do najnowszej dostępnej w dniu wdrożenia i stabilnej wersji (wymaganie to dotyczy również infrastruktury zależnej, współpracującej z wdrażanymi rozwiązaniami).
3. Wymagania w zakresie instalacji i wdrożenia urządzeń klasy UTM:
   3.1. Instalacji Klastrów UTM (Typ 1 oraz Typ 2) we wskazanych punktach dystrybucji okablowania.
   3.2. Wdrożenia Klastrów UTM (Typ 1 oraz Typ 2) do ochrony styku z Internetem wskazanych przez Zamawiającego segmentów sieci, w tym:
   3.3. Konfiguracji interfejsów urządzenia (w tym LACP, VLAN),
   3.4. Konfiguracji routingu IP,
   3.5. Konfiguracji mechanizmów zarządzania,
   3.6. Konfiguracji reguł firewalla,
   3.7. Konfiguracji modułów funkcyjnych (min. IPS, AntiVirus).
4. Wymagania w zakresie instalacji i wdrożenia analizatora logów:
   4.1. Instalacji analizatora logów we wskazanym punkcie dystrybucji okablowania.
   4.2. Konfiguracji logowania zdarzeń z wdrożonego klastra UTM na dostarczony analizator logów.
   4.3. Skonfigurowania we współpracy z Zamawiającym pięciu typów raportów służących do oceny stopnia wykorzystania oraz ochrony styku z Internetem
5. Wymagania w zakresie instalacji i wdrożenia serwera backupu:
   5.1. Instalacja serwera we wskazanej serwerowni i szafie rack.
   5.2. Instalacja oprogramowania do wykonywania kopii zapasowych na serwerze.
   5.3. Instalacja i konfiguracja systemu operacyjnego Microsoft Windows Server na serwerze, podłączenie serwera do wskazanego przez Zamawiającego segmentu sieci.
   5.4. Wymagana rozbudowa środowiska backupu o dodatkowy storage - rozszerzenie środowiska backupu o drugą instancję backupów (backup copy), polegające na wyniesieniu do lokalizacji zewnętrznej względem głównego CPD, w celu realizacji minimalnej rekomendowanej strategii kopii zapasowych „3-2-1”, czyli: przechowuj 3 egzemplarze zasobów – dane produkcyjne, backup i jego replikę;
   5.5. Skonfigurowanie dostarczonego serwera jako serwera kopii zapasowych, w tym zdefiniowanie zadań i harmonogramów kopii zapasowych oraz wykonanie testowego odtwarzania danych dla wskazanych przez Zamawiającego zasobów (serwery fizyczne, wirtualne – w ilości zgodnej z wymaganym licencjonowaniem).
6. Realizacji prac wdrożeniowych musi się odbywać przez osoby posiadające certyfikaty producentów wdrażanych rozwiązań.
7. Realizacji prac wdrożeniowych, które będą skutkowały niedostępnością środowiska IT Zamawiającego, w godzinach 20:00 – 5:00 w dni od poniedziałku do piątku lub w sobotę i niedzielę przez cała dobę i planowane w uzgodnieniu z Zamawiającym z minimum trzydniowym wyprzedzeniem.
8. Rekonfiguracji posiadanego przez Zamawiającego środowiska przetwarzania danych w celu uzyskania optymalnej wydajności i niezawodności, ze szczególnym uwzględnieniem możliwości i parametrów wydajnościowych dostarczonego sprzętu i oprogramowania
9. Opracowania dokumentacji powykonawczej wdrożenia, obejmującej całość wykonanych prac oraz zmiany wprowadzone w infrastrukturze zależnej.
10. Wykonawca w ramach wdrożenia zapewni 30 godzin asysty technicznej po zakończonym wdrożeniu w okresie 6 miesięcy od daty końcowego odbioru. Asysta będzie realizowana w siedzibie Zamawiającego.