



Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA – OPIS TECHNICZNY

**« DOSTAWA OPROGRAMOWANIA I SPRZĘTU NA POTRZEBY
CYBERBEZPIECZEŃSTWA W RAMACH PROJEKTU „CYBERBEZPIECZNY
SAMORZĄD – URZĄD MIASTA RADZYŃ PODLASKI” »**

Spis treści

1.	Oprogramowanie typu NAC.....	2
2.	Oprogramowanie typu DLP.....	7
3.	Urządzenie do retencji oraz analizy logów	11
4.	EDR.....	13
5.	Skaner podatności	30
6.	Serwery dla rozwiązań cyberbezpieczeństwa.....	37
6.1.	<i>Serwer dla rozwiązań cyberbezpieczeństwa – typ 1.....</i>	<i>37</i>
6.2.	<i>Serwer dla rozwiązań cyberbezpieczeństwa – typ 2.....</i>	<i>45</i>
7.	Rozwój zasobów backupowych	47

1. Oprogramowanie typu NAC

	Wymagania minimalne
Opis funkcjonalności rozwiązania	<ol style="list-style-type: none"> 1. Wymagane jest dostarczenie rozwiązania typu NAC (Network Access Control), służącego do monitorowania sieci lokalnych w celu uwidocznienia pracujących w nich urządzeń oraz wykrywania nowych urządzeń pojawiających się w sieci, w czasie rzeczywistym. Rozwiązanie musi raportować aktualny stan każdego urządzenia, z uwzględnieniem takich atrybutów, jak adres MAC, adres IP, nazwa hosta, system operacyjny, itp., pozyskując te informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.). 2. Rozwiązanie ma za zadanie zapewnić, aby tylko urządzenia, których aktualny stan spełnia zdefiniowaną przez administratora politykę bezpieczeństwa, mogły bez ograniczeń ze strony NAC pracować w sieci lokalnej. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenia, których aktualny stan nie spełnia danych warunków polityki bezpieczeństwa (np. nowe, po raz pierwszy pojawiające się urządzenie lub stacja robocza z wyłączonym oprogramowaniem antywirusowym). Mechanizm kwarantanny powinien umożliwiać całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, jak również blokowanie częściowe, w zakresie definiowanym przez administratora (przez wskazanie adresów IP, z którymi urządzenie może się komunikować). Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej. 3. Rozwiązanie musi posiadać funkcjonalność typu Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów.
Wymagania ogólne rozwiązania NAC	<ol style="list-style-type: none"> 4. Ma zapewnić widoczność i monitorowanie wszystkich urządzeń pracujących w sieci lokalnej oraz powiadamiać o nowych urządzeniach pojawiających się w sieci. 5. Musi zapewniać automatyczne blokowanie komunikacji sieciowej między nowym, niezauważanym urządzeniem a zaufanymi, zarządzanymi urządzeniami pracującymi w sieci. 6. Musi umożliwiać sprawdzanie statusu aktualizacji oprogramowania antywirusowego i poprawek systemowych na zarządzanych stacjach roboczych Windows i w przypadku nie spełniania określonych wymagań, automatycznie ograniczać tym stacjom roboczym możliwość pracy w sieci. 7. Musi umożliwiać odbieranie komunikatów bezpieczeństwa z innych systemów bezpieczeństwa (np. firewalla) i automatyczne blokowanie na tej podstawie wskazanych urządzeń w sieci. 8. Musi mieć funkcję wykrywania faktu skanowania urządzeń i portów wykonywanego przez urządzenie w sieci lokalnej i automatycznie blokować takie urządzenie, aby zapobiegać potencjalnemu szerzeniu się malware.

	<p>9. Stosowany mechanizm blokowania musi wykorzystywać protokół ARP i działać całkowicie niezależnie od innych elementów infrastruktury sieciowej.</p> <p>10. Rozwiązanie musi działać bezagentowo, bez konieczności instalowania jakichkolwiek agentów na urządzeniach w sieci oraz bez konieczności dokonywania zmian w infrastrukturze sieciowej.</p> <p>11. Rozwiązanie musi umożliwiać wysyłanie alertów do administratora za pomocą e-maila oraz SMS</p> <p>12. Rozwiązanie musi być zarządzane przez interfejs webowy, obsługiwany przeglądarką internetową</p> <p>13. Wymaga się, aby rozwiązanie było dostarczone w postaci maszyny wirtualnej na platformę VMware oraz Hyper-V. System musi pozwalać na monitorowanie co najmniej 10 sieci VLAN i monitorowanie łącznie co najmniej 100 urządzeń.</p> <p>14. Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej i dostarczone z licencją pozwalającą na monitorowanie 100 urządzeń wraz ze wsparciem technicznym.</p>
Wymagania szczegółowe – monitorowanie podsieci	<p>15. Rozwiązanie musi w czasie rzeczywistym raportować widoczność wszystkich urządzeń pracujących w monitorowanych podsieciach.</p> <p>16. Rozwiązanie musi wykrywać nowe nieznanne urządzenie, dołączające się do sieci LAN lub WLAN, w czasie nie dłuższym, niż 5 sekund oraz wysłać powiadomienie mailowe do administratora</p> <p>17. Rozwiązanie musi wykrywać przypadki skanowania urządzeń i portów w monitorowanych podsieciach i blokować urządzenie inicjujące takie skanowanie</p> <p>18. Rozwiązanie musi określać aktualny stan każdego urządzenia, pozyskując informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.) oraz odświeżać te informacje cyklicznie. Musi być możliwość wykorzystania pozyskanych informacji do definiowania polityk bezpieczeństwa.</p> <p>19. Rozwiązanie musi chronić przed podszywaniem się pod adres MAC (MAC spoofing), umożliwiając zdefiniowanie „odcisku palca” (fingerprint) dla każdego zaufanego urządzenia. Odcisk palca musi być kombinacją co najmniej: adresu MAC, adresu IP, nazwy hosta, nazwy systemu operacyjnego, otwartych portów TCP. Jeśli przeprowadzana cyklicznie weryfikacja odcisku palca wykaże jego zmianę, urządzenie powinno zostać zablokowane.</p> <p>20. Rozwiązanie musi obsługiwać VLANy, tj. umożliwiać monitorowanie przez jeden fizyczny interfejs sieciowy wielu podsieci, zdefiniowanych jako VLANy</p>
Wymagania szczegółowe – polityka bezpieczeństwa	<p>21. Rozwiązanie musi umożliwiać definiowanie polityki bezpieczeństwa, czyli określenie przez administratora, jakie warunki musi spełniać aktualny stan urządzenia, aby uzyskało ono określony dostęp do sieci.</p> <p>22. W definiowaniu polityki bezpieczeństwa musi być możliwość wykorzystania informacji o aktualnym stanie urządzenia, pozyskanych bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.), poprzez integrację z tymi systemami.</p> <p>23. Polityka bezpieczeństwa musi umożliwiać przypisanie do urządzenia jednego z trzech trybów dostępu do sieci:</p> <p>24. pełny dostęp</p> <p>25. blokowanie (całkowity brak dostępu)</p>

	<p>26. ograniczony dostęp</p> <p>27. Zakres ograniczonego dostępu powinien być definiowany przez administratora, np. w postaci list ACL, określających, do których adresów IP i portów urządzenie ma dostęp. Musi być możliwość zdefiniowania wielu różnych zakresów ograniczonego dostępu.</p> <p>28. Rozwiązanie powinno automatycznie sprawdzać, które warunki polityki bezpieczeństwa spełnia urządzenie i na tej podstawie przypisywać do urządzenia właściwy zakres dostępu.</p> <p>29. Zakres dostępu, wynikający ze spełnienia przez urządzenie danych warunków polityki bezpieczeństwa powinien być egzekwowany przez mechanizm kwarantanny.</p> <p>30. Musi być możliwość łatwego, manualnego tworzenia białej listy adresów MAC, czyli listy urządzeń mogących bez żadnych ograniczeń ze strony NAC pracować w sieci.</p>
Wymagania szczegółowe – mechanizm kwarantanny	<p>31. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenie, aby wyegzekwować ograniczenia dostępu do sieci, wynikające z polityki bezpieczeństwa</p> <p>32. Mechanizm kwarantanny powinien umożliwiać:</p> <p>32.1. całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym,</p> <p>32.2. częściowe blokowanie komunikacji urządzenia z otoczeniem sieciowym, w zakresie definiowanym przez administratora przez wskazanie adresów IP i portów, z którymi urządzenie może się komunikować</p> <p>33. Mechanizm kwarantanny powinien blokować komunikację urządzenia w czasie nie dłuższym, niż 5 sekund od zaistnienia warunku, powodującego nałożenie kwarantanny</p> <p>34. Dla urządzeń zaufanych, czyli w polityce bezpieczeństwa spełniających kryteria pełnego dostępu do sieci, rozwiązanie nie powinno w żaden sposób przekierowywać ani blokować komunikacji wychodzącej z tych urządzeń</p> <p>35. Kwarantanna powinna być zdejmowana z urządzenia automatycznie, gdy spełni ono kryteria polityki bezpieczeństwa, pozwalające na pełny dostęp</p> <p>36. Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej, musi być niezależny od stosowanych w sieci przełączników, zarządzalnych bądź niezarządzalnych</p> <p>37. Awaria rozwiązania nie może powodować blokady komunikacji w sieci, tj. w przypadku awarii rozwiązania wszystkie urządzenia mają mieć pełny dostęp do sieci</p> <p>38. Rozwiązanie musi umożliwiać włączenie i wyłączenie mechanizmu kwarantanny (blokowania komunikacji) w każdej monitorowanej podsieci osobno</p>
Wymagania szczegółowe – integracja z systemami zewnętrznymi	<p>39. Rozwiązanie musi umieć sprawdzić, czy urządzenia z systemem Windows są dołączone do domeny AD</p> <p>40. Rozwiązanie powinno umożliwiać sprawdzanie statusu oprogramowania antywirusowego, poprawek systemowych i firewalla bezpośrednio na zarządzanych stacjach roboczych Windows w domenie AD, w sposób bezagentowy, przy użyciu WMI.</p> <p>41. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym poprawkami Windows i sprawdzanie statusu zainstalowanych poprawek na</p>

	<p>zarządzanych urządzeniach z systemem Windows. Wymagana jest możliwość integracji co najmniej z systemami: Microsoft WSUS.</p> <p>42. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym agentami antywirusowymi i sprawdzanie statusu agentów AV zainstalowanych na zarządzanych urządzeniach (co najmniej, czy agent jest zainstalowany, aktywny i ma aktualne sygnatury wirusów). Wymagana jest możliwość integracji co najmniej z systemami: Bitdefender, Carbon Black, CrowdStrike, Cybereason, Eset, FireEye, McAfee, SentinelOne, Sophos, Symantec, TrendMicro, Webroot.</p> <p>43. Rozwiązanie musi umożliwiać wykorzystanie pozyskanych informacji, wymienionych w poprzedzających punktach 1-4, do definiowania polityki bezpieczeństwa.</p> <p>44. Rozwiązanie musi umieć odbierać alerty przysyłane za pomocą e-mail lub syslog z innych urządzeń bezpieczeństwa (np. firewalle) i na podstawie zawartych w nich informacji blokować wskazane podejrzane urządzenie</p>
<p>Wymagania szczegółowe – rejestracja urządzeń zewnętrznych: pracowników, gości i konsultantów (Captive Portal)</p>	<p>45. Rozwiązanie musi posiadać wbudowaną funkcję Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów. NAC musi przekierowywać ruch HTTP/S od nieznanych urządzeń do tego portalu.</p> <p>46. Captive Portal musi umożliwiać pracownikom rejestrowanie urządzeń prywatnych (BYOD) i wnioskowanie o dostęp do sieci w ograniczonym zakresie, zdefiniowanym przez administratora.</p> <p>47. Przy rejestracji przez pracowników ich prywatnych urządzeń, Captive Portal powinien umożliwiać użycie ich kont Active Directory</p> <p>48. Powinna istnieć możliwość ograniczenia ilości i rodzaju rejestrowanych przez pracownika prywatnych urządzeń</p> <p>49. Powinna być możliwość przypisania ograniczonego dostępu dla zarejestrowanych urządzeń prywatnych</p> <p>50. Captive Portal musi umożliwiać osobom nie będącym pracownikami (gościom lub konsultantom) wnioskowanie o ograniczony dostęp do sieci</p> <p>51. W przypadku rejestracji urządzeń gości powinna być możliwość rejestracji samodzielnie przez gościa oraz przez uprawnionego pracownika firmy</p> <p>52. Zarejestrowane urządzenia gości powinny automatycznie tracić przydzielony dostęp po upływie zdefiniowanego czasu</p> <p>53. Powinna istnieć możliwość ograniczenia ilości urządzeń rejestrowanych przez gościa</p> <p>54. Dla zarejestrowanych urządzeń gości powinna być możliwość ograniczenia, w jakich przedziałach czasu i z jakich podsieci będą one miały dostęp do sieci</p> <p>55. Dla urządzeń gości powinna być możliwość przypisania dostępu ograniczonego tylko do dostępu do Internetu</p> <p>56. Dla urządzeń konsultantów powinna być możliwość przypisania dostępu ograniczonego do wybranych zasobów lokalnych</p> <p>57. Rozwiązanie musi umożliwiać zatwierdzenie dostępu dla zarejestrowanego urządzenia gościa i konsultanta drogą mailową. Osoba zatwierdzająca powinna otrzymać z systemu e-mail z wnioskiem o dostęp i udzielić go, odpowiadając na maila lub klikając przygotowany link w treści maila.</p> <p>58. Rozwiązanie musi przechowywać historyczne raporty dostępu do sieci użytkowników typu gość i konsultant</p>

	59. Wygląd Captive Portal musi być edytowalny w zakresie co najmniej zmiany firmowego logo i kolorów oraz informacji, jakie we wniosku rejestracyjnym musi podać gość lub konsultant
Pozostałe wymagania	<p>60. Rozwiązanie powinno oferować możliwość zainstalowania opcjonalnego agenta na zarządzanych stacjach roboczych (wymagane wsparcie dla Windows, Linux i MacOS), który przesyła do serwera zarządzającego NAC szczegółowe informacje na temat stacji roboczej, umożliwiając definiowanie na bazie tych informacji precyzyjnych polityk bezpieczeństwa.</p> <p>61. Rozwiązanie nie powinno pogarszać wydajności pracy przełączników i routerów, nie może wymagać współpracy z przełącznikami przez port mirroring czy port spanning.</p> <p>62. Rozwiązanie nie powinno pogarszać wydajność łącz WAN</p> <p>63. Rozwiązanie nie powinno pogarszać wydajności pracy monitorowanych urządzeń w sieci</p>
Wsparcie techniczne	<p>64. Wymaga się wdrożenia rozwiązania w infrastrukturze Zamawiającego, w zakresie:</p> <p>64.1. instalacji i konfiguracji rozwiązania w maszynie wirtualnej na platformie Zamawiającego,</p> <p>64.2. instruktażu dla administratorów rozwiązania.</p> <p>65. Wymaga się wsparcie w języku polskim w trybie 8 godzin dziennie przez 5 dni w tygodniu (w dni robocze: od poniedziałku do piątku), w tym cykliczne przeglądy konfiguracji rozwiązania tzn. co najmniej raz na trzy miesiące.</p>

2. Oprogramowanie typu DLP

System zabezpieczenia danych przed wyciekami informacji

Wymaga się dostawy kompletnego rozwiązania do ochrony stacji roboczych Windows przed wyciekami danych, pochodzącego od jednego producenta, o minimalnej funkcjonalności opisanej poniżej. Wymagane jest, aby cała funkcjonalność była dostępna w ramach jednej, jednolitej instalacji oferowanego systemu ochrony danych przed wyciekami ze zintegrowanym systemem kontroli portów i szyfrowaniem – całość realizowana w ramach jednego agenta na stacjach roboczych.

Zamawiający wymaga dostarczenia rozwiązania, które spełnia co najmniej następujące minimalne wymagania:

Wymagania ogólne

- 1.1. Rozwiązanie ma chronić dane na stacjach roboczych Windows przed wyciekami, poprzez kontrolę portów fizycznych i podłączanych do nich nośników zewnętrznych oraz przez szyfrowanie danych na dyskach lokalnych i nośnikach zewnętrznych.
- 1.2. Rozwiązanie powinno działać w oparciu o definiowanie polityk bezpieczeństwa i integrować się z Active Directory przez wiązanie polityk bezpieczeństwa z obiektami Active Directory. Wymaga się, aby polityka mogła być powiązana z różnymi rodzajami obiektów AD:
 - 1.2.1. Domena
 - 1.2.2. Jednostka Organizacyjna (OU)
 - 1.2.3. Grupa
 - 1.2.4. Użytkownik
 - 1.2.5. Komputer
- 1.3. Rozwiązanie nie może w żaden sposób modyfikować, usuwać ani tworzyć obiektów w drzewie AD.
- 1.4. Rozwiązanie powinno składać się z pojedynczego serwera zarządzającego, oferującego konsolę administracyjną do zarządzania politykami bezpieczeństwa, konfigurowania i monitorowania pracy systemu oraz z agenta, instalowanego na stacjach roboczych, który egzekwuje polityki bezpieczeństwa przypisane do komputera bądź użytkownika.
- 1.5. Dystrybucja polityk bezpieczeństwa i ich odświeżanie na stacjach roboczych muszą zachodzić automatycznie i cyklicznie z częstotliwością definiowaną przez administratora, ale również z możliwością wymuszonego odświeżenia na żądanie z poziomu konsoli administracyjnej oraz ze stacji roboczej.
- 1.6. Wymaga się, aby polityki bezpieczeństwa były egzekwowane również w trybie „offline”, czyli gdy stacja robocza nie ma kontaktu z serwerem zarządzającym (np. laptop poza firmą).
- 1.7. Wymagane jest dostarczenie pliku instalacyjnego agenta w postaci pakietu MSI, z możliwością dystrybucji tego pakietu co najmniej przez Active Directory GPO lub inne systemy dystrybucji centralnej oprogramowania.
- 1.8. Agent musi być wspierany dla stacji roboczych z biznesową wersją Windows 10/11.

2. Kontrola portów fizycznych i nośników zewnętrznych

- 2.1. Produkt musi umożliwiać całkowite blokowanie użycia portów fizycznych:

- 2.1.1. USB
- 2.1.2. Firewire
- 2.1.3. PCMCIA
- 2.1.4. Secure Digital
- 2.1.5. Serial
- 2.1.6. Paralel
- 2.1.7. Porty wewnętrzne
- 2.1.8. WiFi
- 2.1.9. Bluetooth
- 2.2. Wymagane jest, aby produkt identyfikował i raportował urządzenia podłączane do portów USB stacji roboczych, według typu, producenta, modelu i numeru seryjnego. Funkcja ta jest konieczna, by usprawnić proces definiowania polityk bezpieczeństwa, dotyczących kontroli nośników zewnętrznych. Niezbędna jest możliwość zdalnego przeskanowania stacji roboczych z poziomu konsoli zarządzającej w celu zidentyfikowania podłączanych do nich urządzeń zewnętrznych.
- 2.3. Produkt musi umożliwiać blokowanie wybranych typów urządzeń podłączanych do portu USB, rozróżniając:
 - 2.3.1. Telefony komórkowe
 - 2.3.2. Urządzenia oparte o system Android
 - 2.3.3. Urządzenia oparte o system iOS
 - 2.3.4. Urządzenia PDA
 - 2.3.5. Smart Card
 - 2.3.6. Urządzenia drukujące
 - 2.3.7. Adaptery sieciowe
 - 2.3.8. Urządzenia audio/video
 - 2.3.9. Urządzenia interfejsu HID
 - 2.3.10. Urządzenia do przetwarzania obrazów
 - 2.3.11. Sprzętowe KeyLoggery
- 2.4. Produkt musi posiadać funkcję definiowania "białych list", czyli urządzeń wyjątkowo dopuszczonych do podłączenia, identyfikowanych przez określenie producenta, modelu i numeru seryjnego urządzenia.
- 2.5. Dla zewnętrznych urządzeń pamięci masowej typu: pendrive, napędy CD/DVD, zewnętrzne dyski twarde – musi być możliwość zdefiniowania w polityce bezpieczeństwa mechanizmów:
 - 2.5.1. Blokowanie urządzeń danego typu
 - 2.5.2. Korzystanie w trybie „tylko do odczytu”
 - 2.5.3. Wymuszenie szyfrowania danych na nośniku
 - 2.5.4. Blokowanie możliwości odczytu z nośnika plików określonego typu (np. plików wykonywalnych)
 - 2.5.5. Blokowanie możliwości zapisywania na nośniku plików określonego typu
 - 2.5.6. Rejestrowanie w logach wszystkich zapisów i odczytów z nośnika, również wtedy, gdy stacja pracuje „offline”
- 2.6. Szyfrowanie danych na nośnikach zewnętrznych musi być przezroczyste dla użytkownika i nie wymagać żadnego zarządzania kluczami szyfrującymi. Musi być możliwość zapisania i odczytania danych z zaszyfrowanego nośnika na dowolnej stacji roboczej wyposażonej w agenta oferowanego rozwiązania.

3. Szyfrowanie dysku lokalnego

- 3.1. Wymaga się funkcjonalności szyfrowania danych na dysku lokalnym, inicjowanej tym samym jednolitym mechanizmem, co inne funkcjonalności, tj. przez przypisanie odpowiedniej polityki bezpieczeństwa do stacji roboczej.
- 3.2. Wymagane jest, aby szyfrowaniem objęte były tylko dane użytkowników, bez szyfrowania sektora rozruchowego i plików systemowych Windows. Przypisanie polityki szyfrowania do stacji roboczej powinno spowodować zaszyfrowanie danych na dysku.
- 3.3. Szyfrowanie danych na dyskach lokalnych musi być przezroczyste dla użytkownika i nie wymagać żadnego zarządzania kluczami szyfrującymi. Proces deszyfrowania/szyfrowania musi być realizowany w czasie rzeczywistym przy modyfikacji plików przez użytkownika.
- 3.4. Obsługa szyfrowania musi być realizowana w całości przez agenta oferowanego rozwiązania, bez konieczności korzystania z rozwiązań zewnętrznych.
- 3.5. Wymaga się, aby zaszyfrowane dane były dostępne dla każdego użytkownika, który na stacji roboczej poprawnie zaloguje się na swoje konto domenowe (w zakresie jego uprawnień na poziomie systemu plików).
- 3.6. Wymaga się, aby żadne zaszyfrowane dane nie były dostępne, gdy na stacji roboczej zaloguje się pracownik Helpdesku. Umożliwi to udzielanie wsparcia użytkownikom w zakresie utrzymania systemu operacyjnego, bez ryzyka ujawnienia treści ich danych przechowywanych na stacji roboczej.
- 3.7. Musi być dostępne narzędzie, pozwalające na odszyfrowanie danych z dysku w przypadku, gdy nie da się uruchomić stacji roboczej w normalnym trybie, np. na skutek uszkodzenia systemu operacyjnego. Skorzystanie z narzędzia musi wymagać akceptacji administratora systemu, np. poprzez wygenerowanie jednorazowego kodu/hasła.

4. Pozostałe wymagania

- 4.1. Wymaga się, by produkt zaopatrzony był w funkcje zabezpieczające przed próbami ingerencji użytkowników w działanie agenta:
 - 4.1.1. Odinstalowanie oprogramowania możliwe dzięki hasłu, które zna wyłącznie administrator IT
 - 4.1.2. Ochrona przed użytkownikami posiadającymi uprawnienia administratora, chcącymi usunąć bądź wyłączyć oprogramowanie
 - 4.1.3. Rejestrowanie wszelkich prób manipulacji przez użytkowników (łącznie z usuwaniem logów)
 - 4.1.4. Wszystkie pliki logów muszą być zaszyfrowane przed nieautoryzowanym dostępem i próbą skasowania
 - 4.1.5. Wszystkie połączenia między aplikacją agencją na stacji roboczej a serwerem zarządzającym muszą być zaszyfrowane przy użyciu protokołu SSL
- 4.2. Musi istnieć możliwość czasowego wstrzymania (zawieszenia) ochrony na stacji roboczej, bez konieczności modyfikacji lub usuwania i ponownego przypisywania polityk bezpieczeństwa. Wstrzymanie ochrony musi wymagać akceptacji administratora systemu, np. przez wygenerowanie jednorazowego hasła.
- 4.3. W czasie swojego działania agent na stacji roboczej nie może obciążać zasobów (CPU, RAM, dysk) w stopniu odczuwalnym przez użytkownika i utrudniającym normalną pracę. Dopuszczalne jest większe obciążenie stacji jedynie przy pierwszym szyfrowaniu dysku lokalnego.
- 4.4. Powinna być możliwość zdefiniowania własnej treści komunikatów w języku polskim, wyświetlanych przez agenta na stacji roboczej.

- 4.5. Wymagana jest możliwość instalacji agenta w trybie ukrytym, tj. bez widoczności żadnych ikon i bez wyświetlania jakichkolwiek komunikatów na stacji roboczej.
- 4.6. Rozwiązanie musi posiadać wbudowany mechanizm automatycznego wykonywania backupu swojej konfiguracji i zgromadzonych logów wg harmonogramu zdefiniowanego przez administratora. System musi umożliwiać całkowite odtworzenie serwera zarządzającego z takiego backupu na wypadek awarii, bez konieczności reinstalowania agentów.
- 4.7. Proponowane rozwiązanie musi wspierać instalację na wirtualnej platformie VMware lub Hyper-V i być z nią kompatybilne.
- 4.8. Rozwiązanie musi być uruchomione na wskazanych zasobach Zamawiającego i nie może wymagać żadnych dodatkowych zewnętrznych komponentów, np. zewnętrznych baz danych lub zewnętrznych programów szyfrujących.
- 4.9. Rozwiązanie musi obsłużyć minimum 63 stacji roboczych oraz 7 serwerów
- 4.10. Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej z odnawianym corocznie supportem, zawierającym wsparcie techniczne producenta oraz dostęp do poprawek i nowych wersji.
- 4.11. Wymaga się, aby funkcjonalność szyfrowania dysków lokalnych była licencjonowana osobno od funkcjonalności kontroli portów fizycznych i nośników zewnętrznych, pozwalając na elastyczność w doborze licencji do potrzeb.
- 4.12. Wymaga się dostarczenia licencji wieczystych ze wsparciem technicznym dla funkcjonalności kontroli portów fizycznych i nośników zewnętrznych oraz licencji wieczystych ze wsparciem technicznym dla funkcjonalności szyfrowania dysków lokalnych.

5. Wsparcie techniczne

- 5.1 Wymaga się wdrożenia rozwiązania w infrastrukturze Zamawiającego, w zakresie:
 - 5.1.1. instalacji i konfiguracji rozwiązania w maszynie wirtualnej na platformie Zamawiającego,
 - 5.1.2. instruktażu dla administratorów rozwiązania.
- 5.2 Wymaga się wsparcie w języku polskim w trybie 8 godzin dziennie przez 5 dni w tygodniu (w dni robocze: od poniedziałku do piątku), w tym cykliczne przeglądy tzn. co najmniej raz na trzy miesiące, konfiguracji rozwiązania.

3. Urządzenie do retencji oraz analizy logów

Zamawiający wymaga dostarczenia rozwiązania które spełnia co najmniej następujące minimalne wymagania:

1. Wymagania Ogólne

- 1.1.** Wymagane jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.
- 1.2.** Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi wersje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

2. Interfejsy, Dysk:

- 2.1.** System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 500 GB.

3. Parametry wydajnościowe:

- 3.1.** System musi być w stanie przyjmować minimum 5 GB logów na dzień.
- 3.2.** Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

4. W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

4.1. Logowanie

- 4.1.1.** Podgląd logowanych zdarzeń w czasie rzeczywistym.
- 4.1.2.** Możliwość przeglądania logów historycznych z funkcją filtrowania.
- 4.1.3.** System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
 - 4.1.3.1.** Listę najczęściej wykrywanych ataków.
 - 4.1.3.2.** Listę najbardziej aktywnych użytkowników.
 - 4.1.3.3.** Listę najczęściej wykorzystywanych aplikacji.
 - 4.1.3.4.** Listę najczęściej odwiedzanych stron www.
 - 4.1.3.5.** Listę krajów , do których nawiązywane są połączenia.
 - 4.1.3.6.** Listę najczęściej wykorzystywanych polityk Firewall.
 - 4.1.3.7.** Informacje o realizowanych połączeniach IPSec.
- 4.1.4.** Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
- 4.1.5.** Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
- 4.1.6.** System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

4.2. Raportowanie

W zakresie raportowania system musi zapewniać:

- 4.2.1. Generowanie raportów co najmniej w formatach: PDF, CSV.
- 4.2.2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
- 4.2.3. Funkcję definiowania własnych raportów.
- 4.2.4. Możliwość spolszczenia raportów.
- 4.2.5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przestania wyników na określony adres lub adresy email.

4.3. Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

- 4.3.1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
- 4.3.2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
- 4.3.3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
 - 4.3.3.1. Malware.
 - 4.3.3.2. Aplikacje sieciowe.
 - 4.3.3.3. Email.
 - 4.3.3.4. IPS.
 - 4.3.3.5. Traffic.
 - 4.3.3.6. Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
- 4.3.4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.

4.4. Zarządzanie

- 4.4.1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
- 4.4.2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
- 4.4.3. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

5. Licencje

- 5.1. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

6. Kompatybilność

W celu osiągnięcia odpowiedniego poziomu bezpieczeństwa posiadanych przez Zamawiającego systemów wymaga się dostarczenia Systemu który będzie współpracować z wdrożonym przez Zamawiającego rozwiązaniem w zakresie cyberbezpieczeństwa i nie spowoduje konieczności jego wyłączenia (kompatybilność).

Zamawiający informuję, że posiada urządzenie UTMfortinet.

Dostarczony system powinien być kompatybilne z powyższym UTM.

7. Serwisy i wsparcie techniczne

7.1. Wymaga się wdrożenia rozwiązania w infrastrukturze Zamawiającego, w zakresie:

- 6.1.1 instalacji i konfiguracji rozwiązania w maszynie wirtualnej na platformie Zamawiającego,
- 6.1.2 instruktażu dla administratorów rozwiązania.

6.2 System musi być objęty serwisem producenta upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24 godziny na dobę przez 7 dni w tygodniu.

4. EDR

	Wymagania minimalne
LICENCJA	<p>Wymagane jest dostarczenie:</p> <ol style="list-style-type: none"> 1. Oprogramowanie wraz z licencją. 2. Oprogramowanie musi posiadać wsparcie techniczne producenta oprogramowania. 3. Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji. W ramach wsparcia technicznego zgłaszanie błędów w Oprogramowaniu do serwisu producenta. 4. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.
Ochrona punktów końcowych urządzeń komputerowych	<ol style="list-style-type: none"> 5. Ochrona antywirusowa niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową. 6. Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta. 7. Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EPP i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej. 8. Rozwiązanie dla ochrony antywirusowej stacji roboczych wspiera następujące systemy operacyjne: <ol style="list-style-type: none"> 8.1. Microsoft Windows 10 8.2. Microsoft Windows 11 8.3. MacOS version 14 "Sonoma" 8.4. MacOS version 13 "Ventura" 8.5. MacOS version 12 "Monterey" 9. Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej: <ol style="list-style-type: none"> 9.1. Microsoft Internet Explorer 9.2. Microsoft Edge 9.3. Mozilla Firefox

- 9.4.** Google Chrome
- 9.5.** Safari
- 10.** Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów posiada Polski interfejs użytkownika.
- 11.** Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o system EDR i mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.
- 12.** Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej
 - 12.1.** Oprogramowanie instalowane na stacjach końcowych, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.
 - 12.2.** Agent instalowany na stacjach końcowych posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.
 - 12.3.** Agent instalowany na stacjach końcowych posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
 - 12.4.** Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych.
 - 12.5.** Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.
 - 12.6.** Agent instalowany na stacjach końcowych monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:
 - 1.1.1.** dostęp do pliku;
 - 1.1.2.** tworzenie nowego procesu;
 - 1.1.3.** nawiązywane połączenia sieciowe;
 - 1.1.4.** wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
 - 1.1.5.** zawartość skryptów uruchamianych na monitorowanej stacji.
 - 12.7.** W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.
 - 12.8.** Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łącz sieciowych.
 - 12.9.** Komunikacja agentów instalowanych na stacjach roboczych, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
 - 12.10.** Komunikacja agentów instalowanych na stacjach roboczych, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).

- 12.11.** W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.
- 12.12.** Dane zbierane przez agentów na stacjach końcowych są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
- 12.13.** Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych.
- 12.14.** Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
- 12.15.** Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych w środowisku informatycznym.
- 12.16.** Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
- 12.17.** Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
- 12.18.** Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
- 12.19.** Każda detekcja zawiera co najmniej następujące informacje:
- 12.19.1.** Listę urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
 - 12.19.2.** Data i czas wystąpienia podejrzanych zdarzeń.
 - 12.19.3.** Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
 - 12.19.4.** Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
 - 12.19.5.** Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
 - 12.19.6.** Poziom ryzyka, określający istotność danej detekcji.
 - 12.19.7.** Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).
- 12.20.** Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).
- 12.21.** Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).

- 12.22.** Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
- 12.23.** Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
- 12.24.** Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
- 12.25.** Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
- 12.26.** Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
- 12.27.** Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
- 12.28.** Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
- 12.29.** Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
- 12.30.** Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.
- 12.31.** Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
- 12.32.** Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
- 12.33.** Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
- 12.34.** Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
- 12.35.** Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
- 12.36.** Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.
- 12.37.** Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
- 12.38.** Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.

- 12.39.** Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransomware.
- 12.40.** Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
- 12.41.** Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
- 12.42.** W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
- 12.43.** Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
- 12.44.** Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
- 12.45.** Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
- 12.46.** Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
- 12.47.** Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
- 12.48.** Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
- 12.49.** Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
- 12.50.** Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
- 12.51.** Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
- 12.52.** Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
- 12.53.** Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
- 12.54.** Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.
- 12.55.** Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.

- 12.56.** Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
- 12.57.** Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
- 12.58.** Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
- 12.59.** Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
- 12.60.** Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
- 12.61.** Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
- 12.62.** Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.
- 12.63.** Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
- 12.64.** Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
- 12.65.** Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
- 12.66.** Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
- 12.67.** Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
- 12.68.** Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”.
- 12.69.** Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.
- 12.70.** Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.
- 12.71.** Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.

- 12.72.** Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
- 12.73.** Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.
- 12.74.** Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
- 12.75.** Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.
- 12.76.** Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
- 12.77.** Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
- 12.78.** Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
- 12.79.** Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
- 12.80.** Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
- 12.81.** Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.
- 12.82.** Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamianie skryptów ActiveX i pobierane pliki.
- 12.83.** Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
- 12.84.** Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
- 12.85.** Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
- 12.86.** Użytkownik podczas próby przejścia na witrynę znajdującą się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
- 12.87.** Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
- 12.88.** Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
- 12.89.** W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
- 12.90.** W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny

dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.

- 12.91.** Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
- 12.92.** Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
- 12.93.** Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
- 12.94.** Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
- 12.95.** Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
- 12.96.** Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
- 12.97.** Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
- 12.98.** Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
- 12.99.** Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
- 12.100.** Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
- 12.101.** Moduł aktualizacji aplikacji pełni rolę mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
- 12.102.** Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
- 12.103.** Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
- 12.104.** Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
- 12.105.** W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.

- 12.106.** Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
- 12.107.** Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
- 12.108.** Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
- 12.109.** Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
- 12.110.** System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
- 12.111.** Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
- 12.112.** Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.
- 12.113.** Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
- 12.114.** Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
- 12.115.** Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
- 12.116.** Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
- 12.117.** Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.
- 12.118.** Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
- 12.119.** Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker
- 12.120.** Rozwiązanie pozwala na zdalne wymuszenie procesu szyfrowania dysków systemowych za pomocą funkcji Bitlocker wbudowanej i obsługiwanej przez system Windows.
- 12.121.** W momencie zdalnego uruchomienia procesu szyfrowania za pomocą funkcji Bitlocker administrator posiada możliwość wymuszenia ustanowienia kodu PIN na stacji roboczej, wymaganego do logowania.
- 12.122.** Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.
- 12.123.** Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.

- 12.124.** Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.
- 12.125.** Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)
- 12.126.** W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.
- 12.127.** Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.
- 12.128.** Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.
- 12.129.** Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.
- 12.130.** Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
- 12.131.** Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.
- 12.132.** Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
- 12.133.** Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.
- 12.134.** Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
- 12.135.** Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
- 12.136.** Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.
- 12.137.** Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji.
- 12.138.** Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.
- 12.139.** Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.
- 12.140.** Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.

- 12.141.** Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN
- 12.142.** Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD)
- 12.143.** Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.
- 12.144.** Rozwiązanie pozwala na wygenerowanie pliku za pomocą którego administrator może wywołać zdalne połączenie za pomocą usług Microsoft RDP (Remote Desktop).
- 12.145.** Wygenerowany plik może być otwarty i wykorzystany do zdalnego połączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.
- 13.** Centralna administracja
- 13.1.** Portal zarządzający jest dostępny w języku polskim.
- 13.2.** Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
- 13.3.** W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.
- 13.4.** Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
- 13.5.** Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
- 13.6.** Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
- 13.7.** Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
- 13.8.** Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.
- 13.9.** Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego połączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
- 13.10.** Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.

- 13.11.** Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
- 13.12.** Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
- 13.13.** Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
- 13.14.** Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki.
- 13.15.** Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach dla których dana poprawka została wydana.
- 13.16.** Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
- 13.17.** Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
- 13.18.** Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
- 13.19.** Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
- 13.20.** Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
- 13.21.** Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu EDR, mechanizmów zarządzania podatnościami, ochrony usług Microsoft 365.
- 13.22.** Dodanie klucza licencyjnego skutkuje pojawieniem się dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
- 13.23.** Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
- 13.24.** Profile mogą być przypisane do pojedynczych hostów lub do grup.
- 13.25.** Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.
- 13.26.** W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.
- 13.27.** Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.
- 13.28.** Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.

	<p>13.29. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.</p> <p>13.30. Pliki instalacyjne mają posiadać plików .EXE, .MSI, .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.</p> <p>13.31. Tworzone profile muszą dawać administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.</p> <p>13.32. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.</p> <p>13.33. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.</p> <p>13.34. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.</p> <p>13.35. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.</p> <p>13.36. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji</p>
Moduł wykrywania i reagowania na podejrzanych aktywności na urządzeniach końcowych (XDR)	<p>14. System klasy EDR/XDR zarządzany z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.</p> <p>15. Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta.</p> <p>16. Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o mechanizm zarządzania podatnościami – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.</p> <p>17. Rozwiązanie posiada możliwość instalacji agenta monitorowania na stacjach roboczych z co najmniej następującymi systemami operacyjnymi:</p> <p>17.1. Microsoft Windows 10</p> <p>17.2. Microsoft Windows 11</p> <p>17.3. MacOS 11 "Big Sur"</p> <p>17.4. MacOS 10.15 "Catalina"</p> <p>17.5. MacOS 10.14 "Mojave"</p> <p>17.6. MacOS 10.15 "Catalina"</p> <p>18. Rozwiązanie posiada możliwość instalacji agenta monitorowania na serwerach z co najmniej następującymi systemami operacyjnymi:</p> <p>18.1. Microsoft® Windows Server 2012</p>

- 18.2.** Microsoft® Windows Server 2016
- 18.3.** Microsoft® Windows Server 2019
- 18.4.** Microsoft® Windows Server 2022
- 19.** Wspierane przeglądarki internetowej:
 - 19.1.** Microsoft Edge
 - 19.2.** Mozilla Firefox
 - 19.3.** Google Chrome
 - 19.4.** Safari
- 20.** Rozwiązanie posiada polski interfejs użytkownika centralnej konsoli zarządzania oraz agenta instalowanego na stacji końcowej oraz serwerze.
- 21.** Oprogramowanie instalowane na stacjach końcowych i serwerach, zwane dalej agentem, ma możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku.
- 22.** Agent instalowany na stacjach końcowych i serwerach posiada możliwość instalacji z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory.
- 23.** Agent instalowany na stacjach końcowych i serwerach posiada możliwość ręcznej instalacji, bez wykorzystania zewnętrznych systemów dystrybucji oprogramowania.
- 24.** Oprogramowanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji oprogramowania agenta monitorującego na stacjach końcowych i serwerach.
- 25.** Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.
- 26.** Agent instalowany na stacjach końcowych i serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:
 - 26.1.** dostęp do pliku;
 - 26.2.** tworzenie nowego procesu;
 - 26.3.** nawiązane połączenia sieciowe;
 - 26.4.** wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
 - 26.5.** zawartość skryptów uruchamianych na monitorowanej stacji.
- 27.** W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.
- 28.** Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.
- 29.** Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
- 30.** Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
- 31.** W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są

buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.

- 32.** Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
- 33.** Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzanе zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.
- 34.** Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
- 35.** Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.
- 36.** Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
- 37.** Detale dotyczące detekcji przedstawiane są w postaci drzewa zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii.
- 38.** Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
- 39.** Każda detekcja zawiera co najmniej następujące informacje:
 - 39.1.** Lista urządzeń na których rozwiązanie zarejestrowało podejrzanе zdarzenia.
 - 39.2.** Data i czas wystąpienia podejrzanых zdarzeń.
 - 39.3.** Listę podejrzanых zdarzeń zidentyfikowanych przez rozwiązanie.
 - 39.4.** Opis dla każdego z podejrzanых zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzanе.
 - 39.5.** Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzanе.
 - 39.6.** Poziom ryzyka, określający istotność danej detekcji.
 - 39.7.** Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).
- 40.** Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).
- 41.** Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).
- 42.** Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
- 43.** Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.

44. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
45. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
46. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
47. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
48. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
49. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
50. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.
51. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
52. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
53. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
54. Konsola centralnego zarządzania, oferuje interfejs w języku Polskim.
55. Konsola zarządzająca wyposażona jest w panel kontrolny (dashboard) w którym administrator ma możliwość weryfikacji stanu bezpieczeństwa organizacji.
56. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.
57. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
58. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.
59. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
60. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności, co najmniej dla systemu antywirusowego oraz mechanizmów zarządzania podatnościami.
61. Dodanie klucza licencyjnego skutkuje aktywowaniem dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.

Wsparcie serwisowe	<p>62. System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora.</p> <p>63. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:</p> <p>63.1. Wsparcie telefoniczne świadczone przez wykwalifikowanych pracowników.</p> <p>63.2. Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.</p> <p>63.3. Doradztwo w zakresie konfiguracji.</p> <p>63.4. Zdalne wsparcie techniczne.</p> <p>63.5. Pomoc w zakładaniu zgłoszeń serwisowych u producenta.</p> <p>63.6. Przygotowanie do zdalnej konfiguracji.</p> <p>63.7. Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.</p> <p>63.8. Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.</p> <p>63.9. Minimum dwa razy (nie rzadziej niż raz na trzy miesiące) zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.</p> <p>63.10. Minimum dwa razy (nie rzadziej niż raz na trzy miesiące) zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.</p> <p>Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24 godziny na dobę przez 7 dni w tygodniu przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim.</p>
Wsparcie techniczne	<p>64. Wymaga się wdrożenia rozwiązania w infrastrukturze Zamawiającego, w zakresie:</p> <p>66.1 instalacji i konfiguracji rozwiązania na platformie Zamawiającego,</p> <p>66.2 instruktażu dla administratorów rozwiązania.</p>

5. Skaner podatności

	Wymagania minimalne
LICENCJA	<ol style="list-style-type: none"> 1. W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. 2. Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji. W ramach licencji możliwość zgłaszania błędów w Oprogramowaniu do serwisu producenta. 3. Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych. 4. Dostarczone licencje dla hostów.
Zaawansowany skaner podatności	<ol style="list-style-type: none"> 5. Rozwiązanie zapewnia wykrywanie oraz zarządzanie podatnościami bezpieczeństwa, w środowisku informatycznym. 6. Architektura rozwiązania składa się z systemu zarządzania oraz osobnego, dedykowanego oprogramowania wykonującego skanowania podatności, które jest zarządzane za pomocą jednej centralnej konsoli zarządzania. 7. Dostęp do konsoli centralnego zarządzania odbywa się z poziomu interfejsu WWW, niezależnie od zastosowanej platformy sprzętowej i programowej. 8. Konsola zarządzania jest dostępna w postaci usługi hostowanej na serwerach producenta 9. Konsola zarządzania oferuje dostęp za pomocą następujących wspieranych przeglądarek internetowych: <ol style="list-style-type: none"> 9.1. Microsoft Edge 9.2. Mozilla Firefox 9.3. Google Chrome 9.4. Safari 10. Konsola zarządzająca dostępna jest w języku polskim. 11. Poza językiem polskim konsola wspiera języki: angielski, niemiecki, francuski, hiszpański, fiński, włoski. 12. Logowanie do konsoli umożliwia wykorzystanie mechanizmów wieloskładnikowego uwierzytelniania (2FA) dla kont posiadających dostęp do konsoli zarządzającej. 13. Mechanizm 2FA służący zabezpieczeniu dostępu do konsoli zarządzającej w swoim działaniu wykorzystuje mechanizmy: powiadomień SMS, oraz tokenów jednorazowych generowanych w aplikacjach mobilnych (np. Google Authenticator, Microsoft Authenticator). 14. Konsola wyposażona jest w panel kontrolny, w którym wyświetlane są informacje podsumowujące dotyczące poziomu bezpieczeństwa chronionej organizacji. 15. Rozwiązanie realizuje skanowania podatności za pomocą dedykowanego oprogramowania, instalowanego w środowisku, zarządzanego z poziomu konsoli centralnego zarządzania. 16. Ta sama konsola umożliwia zarządzanie innymi produktami w przypadku posiadania odpowiedniej licencji w tym co najmniej ochrony antymalware, systemem EDR, ochroną usług Microsoft 365

17. Konsola pozwala na podgląd posiadanych licencji oraz ich wykorzystania.
18. Oprogramowanie skanujące podatności bez agentowo (lokalny scan node) dostępne jest w postaci aplikacji instalowanej lokalnie i wspiera poniższe systemy operacyjne:
 - 18.1. Windows Server 2016 i nowsze
 - 18.2. Ubuntu server (wersje 64 bitowe 16.x 18.x, 20.x)
 - 18.3. Debian (wersje 64 bitowe 9,10,11)
19. Rozwiązanie umożliwia również agentowe skanowanie w poszukiwaniu podatności na komputerach z systemem Windows.
20. Agent instalowany na systemach Windows wspiera systemy MS Windows 10 i 11 oraz systemy serwerowe MS Windows Server 2016 i nowsze.
21. Ten sam agent zainstalowany na wspieranych systemach Windows w przypadku posiadania odpowiedniej licencji może dodatkowo zapewniać również ochronę antymalware i funkcjonalność systemu EDR.
22. Skanowanie agentowe odbywać się może w cyklach co:4,6,12,24 godzin
23. Istnieje możliwość włączenia i wyłączenia funkcji skanowania agentowego.
24. Wyłączenie funkcji skanowania agentowego nie powoduje deinstalacji agenta na danym hoście.
25. Rozwiązanie umożliwia przeprowadzenie skanowania, wykrywającego urządzenia pracujące w skanowanej sieci komputerowej.
26. Skanowanie wykrywające urządzenia pracujące w skanowanej sieci umożliwia:
 - 26.1. wykrywanie urządzeń pracujących w skanowanej sieci na podstawie protokołów: ARP, ICMP PING, SSH, HTTP, HTTPS, RDP.
 - 26.2. wykrycie pracujących urządzeń w oparciu o analizę wszystkich dostępnych otwartych portów sieciowych.
 - 26.3. Pozwala na konfigurację parametrów skanowania takich jak:
 - 26.4. zakres przeszukiwanych portów (osobne wartości dla TCP i UDP)
 - 26.5. wydajność skanowania (6 poziomów),
 - 26.6. liczbę jednoczesnych wątków skanowania (1,2,4,8,16,24,32)
 - 26.7. możliwość wykrycia wersji systemu operacyjnego.
 - 26.8. konfigurację harmonogramu uruchamiania skanu (np. dziennie, tygodniowo, w określony dzień miesiąca, kwartalnie oraz wskazanie godziny rozpoczęcia skanowania)
 - 26.9. określenia maksymalnej ilości wykonanych skanowań (1-100) lub bez ograniczenia.
 - 26.10. konfigurację wysyłania powiadomień na wskazane adresy e-mail
 - 26.11. powiadomienia dotyczyć mogą: informacji o rozpoczęciu skanowania, jego zakończeniu, zmiany ilości hostów w stosunku do poprzedniego skanowania, zmiany ilości portów w stosunku do poprzedniego skanowania.
27. Konsola zarządzająca umożliwia podgląd listy skonfigurowanych skanów wykrywających dostępne hosty w sieci, wraz z informacją o zmianach w stosunku do ostatniego przeprowadzonego skanu.
28. Widok listy dostępnych skanowań wykrywających obiekty pozwala na zaawansowane filtrowanie.
29. Konsola pozwala na uruchomienie z poziomu listy dostępnych skanowań, wskazanego skanowania wykrywającego obiekty na żądanie z pominięciem harmonogramu.

30. Trwające zadanie skanowania w poszukiwaniu obiektów może zostać przerwane na żądanie.
31. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego dostępne urządzenia w sieci do pliku XLSX oraz XML.
32. Rozwiązanie umożliwia uruchomienie skanowania wykrywającego znane podatności bezpieczeństwa na urządzeniach sieciowych.
33. Skan wykrywający znane podatności bezpieczeństwa na urządzeniach sieciowych umożliwia:
 - 33.1. określenie skanowanego celu za pomocą adresu IP, oraz grupy celów za pomocą adresu podsieci IP.
 - 33.2. masowe wprowadzenie listy skanowanych celów (adresów IP), za pomocą ustrukturyzowanego pliku z rozszerzeniem CSV.
 - 33.3. konfigurację parametrów skanowania, takich jak:
 - 33.3.1. zakres skanowanych portów sieciowych TCP/UDP,
 - 33.3.2. parametr wydajności skanowania (6 poziomów)
 - 33.3.3. rodzaj uwierzytelniania na skanowanej stacji.
 - 33.3.4. konfigurację harmonogramu uruchamiania skanu: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia.
 - 33.3.5. konfigurację wysyłania powiadomień na wskazane adresy e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu.
34. W przypadku tworzonego zadania skanowania administrator posiada możliwość określenia czy do celu skanowania mają zostać wykorzystane wszystkie dostępne pluginy skanujące, tylko wybrane, wszystkie pluginy poza wskazanymi.
35. Administrator posiada możliwość podglądu dostępnych pluginów skanujących podatności i przeszukiwania ich listy.
36. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających znane podatności bezpieczeństwa.
37. Konsola pozwala na uruchomienie i zatrzymanie skanowania w poszukiwaniu znanych podatności na żądanie.
38. Konsola zarządzania umożliwia eksport wyniku skanu wykrywającego znane podatności bezpieczeństwa do pliku docx i xml
39. Dla danego hosta widoczne są wyniki skanowania w poszukiwaniu podatności.
40. Wyniki zawierają listę wykrytych podatności wraz z poziomem ich krytyczności
41. Dla danej wykrytej podatności dostępny jest: jej opis, poziom krytyczności w oparciu o punktację CVSS, datę wykrycia, wersję pluginu który wykrył podatność, sugestię rozwiązania (jeśli jest dostępna), informację o publicznie dostępnym exploicie (jeśli jest dostępna), zewnętrzne referencje (jeśli są dostępne).
42. Dla wybranych przez administratora wykrytych podatności, w celu ich obsługi istnieje możliwość stworzenia zgłoszenia we wbudowanym w rozwiązanie systemie zgłoszeń.
43. Podczas tworzenia zgłoszenia administrator ma możliwość określenia: nazwy zgłoszenia, wskazania konta osoby, do której zgłoszenie zostanie przypisane, priorytetu, tzw. „deadline” do którego zgłoszenie powinno zostać rozwiązane, dodatkowego opisu.

44. Lista wszystkich stworzonych zgłoszeń wraz z ich statusem widoczna jest z poziomu konsoli zarządzającej.
45. Administrator posiada możliwość sortowania oraz filtrowania stworzonych zgłoszeń.
46. Osoba, dla której zostało przypisane zgłoszenie ma możliwość dodawania komentarzy, w celu informowania o etapach procesu rozwiązywania zgłoszenia.
47. Dla zgłoszenia istnieje możliwość zmiany jego statusu.
48. Rozwiązanie umożliwia uruchomienie skanu wykrywającego luki bezpieczeństwa w aplikacjach webowych.
49. Skanowanie wykrywające luki bezpieczeństwa w aplikacjach webowych umożliwia:
 - 49.1. określenie skanowanego celu za pomocą adresu URL.
 - 49.2. konfigurację parametrów skanowania takich jak:
 - 49.2.1. rodzaje testowanych ataków,
 - 49.2.2. wyjątki ze skanowania (adresy URL omijane podczas testowania aplikacji web),
 - 49.2.3. parametr wydajności skanowania (ilość jednoczesnych zapytań przesyłanych do skanowanej aplikacji).
 - 49.2.4. konfigurację uwierzytelniania w testowanej aplikacji web.
 - 49.2.5. konfigurację harmonogramu uruchamiania skanowania: dziennie, tygodniowo, w określony dzień miesiąca, oraz wskazanie godziny rozpoczęcia skanowania.
 - 49.2.6. konfigurację wysyłania powiadomień na wskazany adres e-mail informujących o momencie rozpoczęcia skanowania oraz jego zakończeniu.
50. Konsola zarządzania umożliwia podgląd listy skonfigurowanych skanów wykrywających luki w aplikacjach webowych
51. Rozwiązanie umożliwia skorzystanie z narzędzia do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet.
52. Narzędzie do identyfikacji zasobów informatycznych dostępnych z publicznej sieci Internet umożliwia:
 - 52.1. przeszukiwanie adresów internetowych, skatalogowanych przez automatyczne systemy producenta, spełniających wskazane warunki wyszukiwania.
 - 52.2. zapisywanie wskazanych warunków wyszukiwania jako szablony.
 - 52.3. podgląd listy wyników wyszukiwania z informacją o wykrytym adresie IP, nazwie oraz słowach kluczowych.
 - 52.4. dodanie wybranych wyników wyszukiwania do grupy skanowania podatności bezpieczeństwa.
53. Rozwiązanie umożliwia podgląd listy wszystkich wykrytych podatności bezpieczeństwa z wszystkich przeprowadzonych skanowań.
54. Lista wszystkich wykrytych podatności musi umożliwiać:
 - 54.1. filtrowanie podatności ze względu na ich rodzaj, przypisany znacznik (tag), urządzenie sieciowe na którym została znaleziona podatność, stopień zagrożenia, status jego naprawy.
 - 54.2. wyświetlenie szczegółów poszczególnych podatności bezpieczeństwa wraz z informacjami na jakich urządzeniach sieciowych dana podatność została wykryta.

	<p>54.3. eksport listy urzędzeń na których została wykryta dana podatność bezpieczeństwa do pliku CSV.</p> <p>55. Rozwiązanie umożliwia utworzenie nowego raportu podsumowującego.</p> <p>56. Rozwiązanie umożliwia podgląd listy wygenerowanych raportów</p> <p>57. Raport podsumowujący umożliwia:</p> <p>57.1. konfigurację szablonu jaki będzie wykorzystany do przygotowania raportu,</p> <p>57.2. wybranie grup urzędzeń, które będą znajdowały się w raporcie,</p> <p>57.3. wybranie poszczególnych statusów oraz poziomu zagrożenia podatności, które będą znajdowały się w raporcie,</p> <p>57.4. Utworzenie harmonogramu generowania raportu</p> <p>57.5. Wskazanie adresu email na który zostanie wysłany link udostępniający wygenerowany raport, wraz z określeniem czasu ważności linku</p> <p>58. Lista wygenerowanych raportów musi umożliwiać:</p> <p>58.1. Wygenerowanie raportu na żądanie</p> <p>58.2. eksport wyniku raportu do pliku XML(pogrupowany hostami), DOCX(pogrupowany hostami lub wykrytymi podatnościami lub podsumowujący), XLSX (pogrupowany wykrytymi podatnościami)</p> <p>59. Administrator ma możliwość określenia: strefy czasowej dla swojej organizacji, długości przetrzymywania raportów (miesiąc, kwartał, pół roku, rok, 2 lata)</p> <p>60. Dostęp do konsoli może być ograniczony na podstawie adresów IP lub ich zakresu.</p>
<p>Moduł sztucznej inteligencji (GenAI) do zarządzania incydentami oraz rozszerzone usługi wsparcia technicznego</p>	<p>61. Monitorowanie krytycznych wykryć skanera podatności oraz modułów EDR/XDR przez certyfikowanych ekspertów producenta oprogramowania</p> <p>62. Walidacja i dochodzenie czy wykrycia są prawdziwe oraz czy wymagają natychmiastowej akcji by zatrzymać incydent, bądź czy są fałszywymi wykryciami</p> <p>63. Eskalacja incydentu do adekwatnego reprezentanta klienta mającego możliwość i autorytet aby odpowiedzieć na incydent</p> <p>64. Porada ekspertów jak zatrzymać i naprawić incydent – na przykład, rekomendując izolację systemów bądź zatrzymanie złośliwych procesów</p> <p>65. Przygotowywanie raportów dla klienta wraz z sugestiami rozwiązań.</p> <p>66. Zawartość raportu : Szczegóły raportu, Przegląd podatności, Podsumowanie podatności, Lista podatności (według podatności i hosta) z opcjami Wglądu, Podsumowania, Wykrywania, Odniesień i Ograniczenia tekstu do 500 znaków.</p> <p>67. Filtrowanie: Selektywne raportowanie podatności (pełne i niestandardowe) i wykluczenia, Uwzględnione systemy operacyjne, Filtry zasobów, Filtry podatności</p> <p>68. Możliwość tworzenia "raportów skróconych" wysyłanych w sposób podsumowujący. Częstotliwość raportów w trybie miesięcznym (minimum raz w miesiącu). Raporty dostarczane kanałem e-mail lub w inny bezpieczny sposób komunikacji ustalony z Zamawiającym.</p> <p>69. System musi zawierać zaawansowany moduł wykorzystujący generatywną sztuczną inteligencję (GenAI) do wspierania zespołów IT i cyberbezpieczeństwa w zarządzaniu incydentami bezpieczeństwa. Integruje się z platformami chmurowymi, oferując funkcjonalności związane z analizą zagrożeń, raportowaniem oraz asystowaniem w dochodzeniach bezpieczeństwa.</p> <p>70. Asystent dochodzeniowy</p>

	<p>70.1. Analizuje wykrycia w szerokim kontekście, integrując dane z różnych źródeł.</p> <p>70.2. Dostarcza czytelne raporty i rekomendacje w języku użytkownika.</p> <p>70.3. Integruje informacje zewnętrzne o zagrożeniach w czasie rzeczywistym.</p> <p>70.4. Automatyzuje proces analizy incydentów, skracając czas reakcji zespołu bezpieczeństwa.</p> <p>71. Asystent świadomości bezpieczeństwa</p> <p>71.1. Generuje cotygodniowe raporty dotyczące zdarzeń bezpieczeństwa.</p> <p>71.2. Raporty zawierają podsumowanie incydentów i zalecane działania.</p> <p>71.3. Zapewnia interaktywny dostęp do szczegółowych danych, umożliwiając szybką weryfikację zagrożeń.</p> <p>71.4. Obsługuje wielojęzyczność, dostarczając raporty w lokalnym języku użytkownika.</p> <p>72. Integracja i kompatybilność</p> <p>72.1. System musi być w pełni zintegrowany z platformą chmurową.</p> <p>72.2. Powinien umożliwiać automatyczne zbieranie, analizowanie i raportowanie zdarzeń.</p> <p>72.3. Musi wspierać wieloplatformowe środowiska IT, w tym systemy Windows, macOS oraz Linux.</p> <p>73. Wymagania dotyczące AI</p> <p>73.1. System powinien wykorzystywać generatywną sztuczną inteligencję do analizy zagrożeń.</p> <p>73.2. Musi zapewniać predefiniowane opcje podpowiedzi minimalizujące ryzyko błędnych rekomendacji.</p> <p>73.3. Powinien umożliwiać uczenie maszynowe na podstawie wcześniejszych incydentów w celu optymalizacji przyszłych działań.</p> <p>74. Bezpieczeństwo danych i prywatność</p> <p>74.1. Dane użytkowników nie mogą być wykorzystywane do trenowania modeli AI poza organizacją.</p> <p>74.2. System musi działać zgodnie z RODO (GDPR) i posiadać mechanizmy ochrony prywatności.</p> <p>74.3. Dostęp do danych musi być regulowany poprzez mechanizmy autoryzacji i kontroli dostępu.</p> <p>75. Raportowanie i analiza</p> <p>75.1. System powinien generować automatyczne raporty w formacie tekstowym i wizualnym.</p> <p>75.2. Raporty powinny obejmować historię incydentów oraz rekomendacje działań naprawczych.</p> <p>76. Powinien umożliwiać eksport danych do systemów SIEM oraz integrację z innymi narzędziami analitycznymi.</p>
<p>Kompatybilność rozwiązania</p>	<p>77. W celu osiągnięcia odpowiedniego poziomu bezpieczeństwa posiadanych przez Zamawiającego systemów wymaga się dostarczenia Systemu który będzie współpracować z wdrożonym przez Zamawiającego rozwiązaniem w zakresie cyberbezpieczeństwa i nie spowoduje konieczności jego wyłączenia (kompatybilność).</p> <p>Zamawiający wymaga, żeby dostarczony System był kompatybilny z dostarczonym EDR.</p>

Rozszerzone wsparcie serwisowe	<p>78. System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora.</p> <p>79. System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:</p> <p>79.1. Wsparcie telefoniczne świadczone przez wykwalifikowanych pracowników.</p> <p>79.2. Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.</p> <p>79.3. Doradztwo w zakresie konfiguracji.</p> <p>79.4. Zdalne wsparcie techniczne.</p> <p>79.5. Pomoc w zakładaniu zgłoszeń serwisowych u producenta.</p> <p>79.6. Przygotowanie do zdalnej konfiguracji.</p> <p>79.7. Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.</p> <p>79.8. Minimum 5 zdalnych rekonfiguracji urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.</p> <p>79.9. Minimum dwa razy (nie rzadziej niż raz na trzy miesiące) zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.</p> <p>79.10. Minimum dwa razy (nie rzadziej niż raz na trzy miesiące) zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.</p>
Wsparcie techniczne	<p>80. Wymaga się wdrożenia rozwiązania w infrastrukturze Zamawiającego, w zakresie:</p> <p>81. instalacji i konfiguracji rozwiązania na platformie Zamawiającego,</p> <p>82. instruktażu dla administratorów rozwiązania.</p>

6. Serwery dla rozwiązań cyberbezpieczeństwa

6.1. Serwer dla rozwiązań cyberbezpieczeństwa - typ 1

Parametr	Charakterystyka (wymagania minimalne)
Typ urządzenia	1. Komputer Serwer z systemem operacyjnym.
Zastosowanie	2. Serwer będzie wykorzystywany na potrzeby cyberbezpieczeństwa w Urzędzie.
Wydajność	3. Procesor wielordzeniowy (jeden lub więcej) zaprojektowany do pracy w komputerach typu serwer, który uzyskuje wynik co najmniej 50000 punktów w teście PassMark – CPU Mark, według wyników opublikowanych na stronie internetowej http://www.cpubenchmark.net/cpu_list.php . Wynik w okresie nie wcześniej niż 21 dni przed terminem składania ofert.
Obudowa	4. Obudowa Rack o wysokości 2U 5. 12 wnęk na dyski 3.5” 6. 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 7. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	8. Płyta główna z możliwością zainstalowania do dwóch procesorów. 9. Obsługa procesorów 32 rdzeniowych. 10. Na płycie głównej powinno znajdować się co najmniej 16 slotów przeznaczonych do instalacji pamięci. 11. Płyta główna powinna obsługiwać co najmniej 1TB pamięci RAM.
Chipset	12. Dedykowany do pracy w serwerach dwuprocesorowych
Pamięć operacyjna	13. Zainstalowana pamięć o pojemności co najmniej 128 GB.
Kontroler RAID	14. Sprzętowy kontroler dyskowy, posiadający 14.1. Min. 8GB nieulotnej pamięci cache, 14.2. Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. 14.3. Wsparcie dla dysków samoszyfrujących
Dyski twarde	15. Zainstalowane: 15.1. 2x dysk SSD o pojemności min. 480GB, Hot-Plug 15.2. 2x dysk SSD SAS o pojemności min. 1.9TB, Hot-Plug 16. Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Gniazda PCI	17. Cztery sloty PCIe

Interfejsy sieciowe/FC/SAS	18. Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Wbudowane porty	19. 4 porty USB w tym min: 19.1. 1 port USB 3.0 z tyłu obudowy, 19.2. 1 port micro USB z przodu obudowy 20. 2 port VGA z czego jeden z przodu obudowy 21. Możliwość rozbudowy o port RS232
Video	22. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	23. Redundantne, Hot-Plug
Zasilacze	24. Redundantne, Hot-Plug min. 700W klasy Titanium
Elementy montażowe	25. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
Bezpieczeństwo	26. Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. 27. 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. 28. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. 29. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła 30. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. 31. Moduł TPM 2.0 znajdujący się bezpośrednio w płycie głównej. Nie dopuszcza się zastosowania modułu wpinanego w płytę główną. 32. Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera 33. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem 34. 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).
Karta Zarządzania	35. Niezależna karta zarządzająca od zainstalowanego na serwerze systemu operacyjnego posiadającej dedykowany port RJ-45 Gigabit Ethernet umożliwiającej: 35.1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej 35.2. szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika 35.3. możliwość podmontowania zdalnych wirtualnych napędów 35.4. wirtualną konsolę z dostępem do myszy, klawiatury 35.5. wsparcie dla IPv6 35.6. wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH

	<p>35.7. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.</p> <p>35.8. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer</p> <p>35.9. integracja z Active Directory</p> <p>35.10. możliwość obsługi przez ośmiu administratorów jednocześnie</p> <p>35.11. Wsparcie dla automatycznej rejestracji DNS</p> <p>35.12. wsparcie dla LLDP</p> <p>35.13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej</p> <p>35.14. możliwość podłączenia lokalnego poprzez złącze RS-232.</p> <p>35.15. możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy.</p> <p>35.16. Monitorowanie zużycia dysków SSD</p> <p>35.17. możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,</p> <p>35.18. Automatyczne zgłaszanie alertów do centrum serwisowego producenta</p> <p>35.19. Automatyczne update firmware dla wszystkich komponentów serwera</p> <p>35.20. Możliwość przywrócenia poprzednich wersji firmware</p> <p>35.21. Możliwość eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON</p> <p>35.22. Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych</p> <p>35.23. Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.</p> <p>35.24. Możliwość wykrywania odchyłeń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera.</p> <p>36. Karta powinna umożliwiać rozszerzenie funkcjonalności o:</p> <p>36.1. możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych</p> <p>36.2. kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania</p> <p>36.3. Automatyczne odświeżanie certyfikatów SSL</p> <p>36.4. możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielokrotnego przy logowaniu do karty zarządzającej</p> <p>36.5. możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień</p> <p>36.6. możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera</p> <p>36.7. możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer</p> <p>36.8. możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe</p> <p>36.9. monitorowanie przepływu powietrza na bieżąco</p>
Oprogramowanie do zarządzania	<p>37. Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</p> <p>37.1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych</p> <p>37.2. integracja z Active Directory</p>

- 37.3.** Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
- 37.4.** Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
- 37.5.** Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram
- 37.6.** Szczegółowy opis wykrytych systemów oraz ich komponentów
- 37.7.** Możliwość eksportu raportu do CSV, HTML, XLS, PDF
- 37.8.** Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
- 37.9.** Grupowanie urządzeń w oparciu o kryteria użytkownika
- 37.10.** Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
- 37.11.** Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
- 37.12.** Szybki podgląd stanu środowiska
- 37.13.** Podsumowanie stanu dla każdego urządzenia
- 37.14.** Szczegółowy status urządzenia/elementu/komponentu
- 37.15.** Generowanie alertów przy zmianie stanu urządzenia.
- 37.16.** Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
- 37.17.** Integracja z service desk producenta dostarczonej platformy sprzętowej
- 37.18.** Możliwość przejęcia zdalnego pulpitu
- 37.19.** Możliwość podmontowania wirtualnego napędu
- 37.20.** Kreator umożliwiający dostosowanie akcji dla wybranych alertów
- 37.21.** Możliwość importu plików MIB
- 37.22.** Przesyłanie alertów „as-is” do innych konsol firm trzecich
- 37.23.** Możliwość definiowania ról administratorów
- 37.24.** Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- 37.25.** Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
- 37.26.** Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
- 37.27.** Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
- 37.28.** 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.
- 37.29.** Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.
- 37.30.** Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
- 37.31.** Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
- 37.32.** Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.

	<p>37.33. Zdalne uruchamianie diagnostyki serwera.</p> <p>37.34. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.</p> <p>37.34.1. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.</p>
Oprogramowanie do monitorowania	<p>Oparta na chmurze aplikacja, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <p>38. Monitoring:</p> <p>38.1. ilość podłączonych oraz rozłączonych systemów</p> <p>38.2. stan podłączonych urządzeń</p> <p>38.3. informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów</p> <p>38.4. Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia</p> <p>38.5. informacje o statusie gwarancji dla poszczególnych urządzeń</p> <p>38.6. informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń</p> <p>38.7. informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.</p> <p>38.8. Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych</p> <p>38.9. 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.</p> <p>38.10. Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.</p> <p>38.11. Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.</p> <p>38.12. Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.</p> <p>38.13. Monitoring parametrów serwerów z informacją o minimum:</p> <p>38.13.1. Obciążeniu procesora</p> <p>38.13.2. Zużyciu pamięci RAM</p> <p>38.13.3. Temperaturze procesorów</p> <p>38.13.4. Temperaturze powietrza wlotowego</p> <p>38.13.5. Zużyciu prądu</p> <p>38.13.6. Zmianach w fizycznej konfiguracji serwera</p> <p>38.13.7. Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.</p> <p>38.14. Monitoring parametrów pamięci masowych z informacją o minimum:</p> <p>38.14.1. Opóźnieniach</p> <p>38.14.2. IOPS</p> <p>38.14.3. Przepustowości</p> <p>38.14.4. Utylizacji kontrolerów</p> <p>38.14.5. Pojemność całkowita i dostępna</p> <p>38.14.6. Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.</p>

- 38.14.7.** Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- 38.14.8.** Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata
- 38.14.9.** Informacje o poziomie redukcji danych
- 38.14.10.** Informacje o statusie replikacji oraz snapshotów
- 38.15.** Monitoring parametrów przełączników sieciowych z informacją o minimum:
 - 38.15.1.** Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny
 - 38.15.2.** Stanie komponentów: zasilacze, wentylatory
 - 38.15.3.** Podłączonych hostach
 - 38.15.4.** Ilości i statusu portów
 - 38.15.5.** Utylizacji procesora
 - 38.15.6.** Utylizacji poszczególnych portów
 - 38.15.7.** Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
- 39.** Aktualizacja firmware
 - 39.1.** możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania
 - 39.2.** możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania
 - 39.3.** możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania
 - 39.4.** możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania
 - 39.5.** możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
- 40.** Raporty
 - 40.1.** Możliwość generowania raportów dla serwerów zawierających informację o:
 - 40.1.1.** Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej
 - 40.1.2.** Średnim obciążeniu: procesorów, pamięci RAM, IO,
 - 40.2.** Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:
 - 40.2.1.** 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
 - 40.3.** Generowanie raportów do plików CSV i PDF
- 41.** Cyberbezpieczeństwo
 - 41.1.** 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.

	<p>41.2. Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.</p> <p>41.3. Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.</p> <p>41.4. Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.</p> <p>42. Wirtualny asystent</p> <p>42.1. 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;</p> <p>43. Możliwość rozszerzenia funkcjonalności</p> <p>43.1. Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.</p> <p>44. Inne</p> <p>44.1. Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android</p> <p>45. Certyfikaty</p> <p>45.1. Oferowana platforma musi być zaprojektowana zgodnie ze standardami:</p> <p>45.1.1. ISO 27001 lub równoważne</p> <p>45.1.2. NIST Security and Privacy Controls for Federal Information Systems and Organization</p> <p>45.2. CSA Cloud Control Matrix</p>
Niezawodność/jakość wytwarzania	<p>46. Certyfikat ISO 9001 lub równoważny dla producenta sprzętu.</p> <p>47. Deklaracja zgodności CE lub równoważne.</p>
Gwarancja producenta	<p>48. Minimum trzyletnia gwarancja producenta, obejmująca wszystkie komponenty komputera. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.</p> <p>49. Dedykowany numer telefonu oraz adres email lub portal techniczny (dokładny adres strony internetowej) producenta umożliwiający zgłaszanie awarii i uzyskania informacji produktowej, w tym konfiguracji fabrycznej oferowanego sprzętu.</p> <p>50. Dostęp do aktualnych sterowników zainstalowanych na serwerze urządzeń realizowany poprzez podanie identyfikatora klienta lub modelu komputera lub numeru seryjnego, na dedykowanej przez producenta stronie internetowej, nawet po wygaśnięciu okresu gwarancji.</p>
System operacyjny + 65 punktów dostępowych per użytkownik	<p>51. System operacyjny odpowiedni dla komputerów typu serwer, w wersji odpowiedniej dla jednostki samorządu terytorialnego, dedykowany dla środowisk wirtualizacyjnych i chmurowych, spełniający co najmniej następujące wymagania:</p> <p>51.1. System dedykowany dla środowisk wirtualizacyjnych i chmurowych klasy enterprise.</p> <p>51.2. Wirtualizacja: Możliwość uruchomienia nielimitowanej liczby maszyn wirtualnych (VM) oraz nielimitowanej liczby kontenerów na wybranej platformie wirtualizacyjnej, z pełnym wsparciem dla kontenerów i ich zarządzania w systemie operacyjnym.</p> <p>51.3. Klastry i skalowalność: Obsługa klastrów do 64 węzłów i 8 000 VM, wsparcie do 48 TB RAM i 2 048 logicznych procesorów na serwer.</p> <p>51.4. Zarządzanie: Centralne zarządzanie, monitorowanie i automatyzacja zadań administracyjnych.</p>

	<p>51.5. Bezpieczeństwo oparte na:</p> <ul style="list-style-type: none"> - technologii wirtualizacji, które wykorzystują izolację sprzętową i wirtualną do ochrony krytycznych zasobów systemowych oraz zapobiegania atakom typu malware, rootkitom i innym zagrożeniom cybernetycznym. Technologia ta powinna zapewniać warstwę izolacji na poziomie sprzętu i oprogramowania, umożliwiając bezpieczne uruchamianie wrażliwych procesów w oddzielnym środowisku wirtualnym. Celem jest zabezpieczenie kluczowych komponentów systemu operacyjnego, takich jak zarządzanie pamięcią, przechowywanie kluczy kryptograficznych, a także zapewnienie bezpiecznego uruchamiania aplikacji i usług, minimalizując ryzyko naruszenia integralności systemu w przypadku udanych ataków złośliwego oprogramowania; - rozwiązaniu do ochrony maszyn wirtualnych, które wykorzystuje technologie zapewniające bezpieczne uruchamianie i izolację maszyn wirtualnych (VM) w środowisku chmurowym lub wirtualnym, chroniąc je przed nieautoryzowanym dostępem, manipulacjami i atakami. Technologie te powinny zapewniać zaawansowane mechanizmy ochrony, takie jak szyfrowanie dysków maszyn wirtualnych, integrację z modułami bezpieczeństwa sprzętowego (np. TPM, HSM), oraz blokowanie dostępu do krytycznych zasobów maszyny wirtualnej przez nieautoryzowane procesy lub użytkowników. Systemy te muszą wspierać uruchamianie maszyn wirtualnych w "izolowanych" środowiskach, które są odporne na próby manipulacji, w tym zmiany konfiguracji sprzętu lub oprogramowania. Technologie ochrony maszyn wirtualnych powinny zapewniać integralność i bezpieczeństwo środowiska wirtualnego, minimalizując ryzyko ataków, które mogą zagrozić danym przechowywanym w maszynach wirtualnych lub samej maszynie wirtualnej. <p>51.6. Sieciowość: Wsparcie dla SDN (Software-Defined Networking) oraz równoważnych rozwiązań sieciowych.</p> <p>51.7. Integracja z chmurą: Możliwość współpracy z hybrydowymi środowiskami chmurowymi.</p> <p>51.8. Licencja + 65 licencji dostępowych które można przypisać odpowiednio do użytkownika, umożliwiające pełne wykorzystanie wirtualizacji i chmury.</p> <p>51.9. Możliwość uruchomienia programów 64 bitowych.</p> <p>51.10. Wymagana licencja na wszystkie rdzenie procesorowe zainstalowane w serwerze.</p> <p>51.11. Oferowany system operacyjny powinien być nieużywany tzn. klucz systemu nie może być wykorzystany wcześniej do aktywacji na innym urządzeniu.</p>
Wsparcie techniczne	<p>52. Wymaga się wdrożenia urządzenia wraz z oprogramowaniem w infrastrukturze Zamawiającego, w zakresie:</p> <p>53. - instalacji i konfiguracji urządzenia wraz z oprogramowaniem w infrastrukturze Zamawiającego,</p> <p>54. - instruktażu dla administratorów rozwiązania.</p>

6.2. Serwer dla rozwiązań cyberbezpieczeństwa - typ 2

Parametr	Charakterystyka (wymagania minimalne)
Typ urządzenia	1. Serwer NAS (Network Attached Storage – sieciowa pamięć masowa).
Zastosowanie	2. Urządzenia do przechowywania danych i tworzenia kopii zapasowych. Działający jako serwer baz danych, serwer FTP, serwer plików, serwer VPN.
Procesor	3. Wielordzeniowy procesor o architekturze 64-bitowej.
Obudowa	4. Typu rack o wysokości maksymalnie 2U wraz z szynami przesuwными umożliwiającymi montaż w szafie rack w zestawie.
Pamięć RAM	5. Zainstalowana pamięć o pojemności 16GB (2 x 8GB).
Liczba obsługiwanych dysków	6. Minimum 12 dysków o maksymalnej pojemności nie mniejszej niż 8TB każdy, po podłączeniu modułów rozszerzających minimum 24 dyski.
Zainstalowane dyski	7. 12 dysków o pojemności 8 TB każdy zgodnych z listą kompatybilności oferowanego serwera z możliwością aktualizacji oprogramowania dysku bezpośrednio z poziomu systemu operacyjnego serwera NAS.
Interfejsy sieciowe	8. Minimum 2 porty 1GbE RJ-45. 9. Minimum 1 port 10GbE RJ-45. 10. Minimum 2 porty 10GbE SFP+. 11. Obsługa agregacji łączy.
Porty	12. Minimum 2 porty USB 3.2. 13. Minimum 1 gniazdo rozszerzenia służące do podłączania jednostek rozszerzających.
Wskaźniki LED	14. Status, HDD, zasilanie, LAN
Obsługa RAID	15. Podstawowy, RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare.
Funkcje RAID	16. Możliwość zwiększania pojemności poprzez wymianę dysków na większe. Migracja poziomu RAID w trybie online dla minimum RAID 1 i RAID 5.
Szyfrowanie	17. Możliwość szyfrowania wybranych udziałów sieciowych.
Protokoły	18. SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP
Usługi	19. Serwer VPN, Serwer pocztowy, Stacja monitoringu, Windows ACL, Integracja z Windows Active Directory, Firewall, Serwer plików, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Usługa DDNS, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów. 20. Wykonywanie kopii zapasowych maszyn wirtualnych ze środowisk takich jak VMware vSphere, VMware free ESXi oraz Microsoft Hyper-V 2016 i 2019 (wraz z klastrami przełączania awaryjnego) z wykorzystaniem centralnego panelu zarządzania oraz dodatkowo: 20.1. Obsługa wszystkich typów i wersji sprzętu wirtualnego VMware, w tym 62TB VMDK. 20.2. Obsługa maszyn wirtualnych Hyper-V generacji 1 i 2, w tym dysków VHDX o pojemności 64 TB i wersji sprzętu wirtualnego od 5.0 do 9.0.

	<p>20.3. W przypadku tworzenia kopii zapasowych Microsoft Hyper-V wymagany jest wolumin systemowy hosta z co najmniej 512 MB wolnego miejsca w celu zainstalowania narzędzia do przenoszenia danych.</p> <p>20.4. Kopia zapasowa oparta na obrazie tworzy kopie zapasowe całych urządzeń, w tym konfiguracji danych i systemu.</p> <p>20.5. Kopia zapasowa bez agentów.</p> <p>20.6. Korzystanie z funkcji VMware Changed Block Tracking i funkcji Hyper-V Resilient Change Tracking do wykonywania przyrostowej kopii zapasowej</p> <p>20.7. Okno kopii zapasowej umożliwiające dostosowywanie dozwolonego i niedozwolonego czasu tworzenia kopii zapasowych.</p> <p>20.8. Metody przywracania: Przywracanie całego urządzenia, przywracanie na poziomie plików/folderów i natychmiastowe przywracanie do VMware vSphere, Microsoft Hyper-V lub wbudowanego wirtualizatora na serwerze NAS.</p> <p>20.9. W przypadku przywracania na poziomie plików w systemie operacyjnym gościa obsługiwane systemy plików systemu Windows to NTFS i FAT32, a obsługiwane systemy plików systemu Linux to NTFS, FAT32, ext3, i ext4.</p> <p>20.10. Kopia zapasowa uwzględniająca aplikacje dla maszyn wirtualnych VMware vSphere lub Microsoft Hyper-V działających w systemie Microsoft Windows 2003 SP1 lub nowszym (z wyjątkiem Nano Server z powodu braku architektury VSS).</p> <p>20.11. Obsługa tworzenia kopii zapasowych systemów operacyjnych i aplikacji obsługiwanych przez rozwiązania VMware vSphere i Microsoft Hyper-V.</p> <p>21. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora.</p>
Obsługa migawek	22. Liczba migawek folderu współdzielonego: minimum 1000
Zarządzanie dyskami	23. SMART, sprawdzanie złych sektorów.
Język GUI	24. Polski
Gwarancja	25. Minimum 36 miesięcy gwarancji producenta, obejmująca wszystkie komponenty serwera.
Certyfikaty	26. Deklaracja zgodności CE lub równoważne.
System plików	27. Dyski wewnętrzne: BTRFS
Szyfrowanie	28. Mechanizm szyfrowania sprzętowego
Zasilacz	29. Redundantny zasilacz o mocy minimum 300W.
Chłodzenie	30. Minimum 3 wentylatory z możliwością regulowania prędkości obrotowej oraz wymiany w urządzeniu podczas pracy.

7. Rozwój zasobów backup'owych

Lp.	Charakterystyka (wymagania minimalne)
1.	Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych.
2.	Dostarczone urządzenie musi oferować przestrzeń min. 16TB netto powierzchni użytkowej bez uwzględniania mechanizmów protekcji – przestrzeń dedykowana do gromadzenia deduplikatów, wymagana skalowalność do min. 170TB netto (powierzchni użytkowej widocznej po założeniu systemu plików)
3.	Dostarczone urządzenie powinno umożliwiać rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityką retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemieszczane (w postaci zdeduplikowanej) na dodatkową warstwę, wymagane wsparcie dla AWS, Microsoft Azure oraz Google GCP. Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń min. 60TB netto dla warstwy CLOUD.
4.	Oferowane urządzenie musi posiadać minimum: <p>4.1. 4-y porty 10Gb/s Eth BaseT wymagana możliwość obsługi każdym z ww. portów protokołów CIFS, NFS, deduplikacja na źródle wymagana możliwość dodania do ww. konfiguracji portów:</p> <p>4.2. 2-a porty FC 16Gb/s wymagana możliwość obsługi poprzez porty FC protokołów VTL oraz deduplikacja na źródle (możliwość dodania dwóch portów FC oznacza oficjalnie wsparcie takiej konfiguracji przez producenta urządzenia, wolny slot na dodatkową kartę HBA w przypadku oferowanej konfiguracji urządzenia oraz możliwość natychmiastowego zamówienia u producenta wymaganej karty rozszerzeń)</p>
5.	Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: <p>5.1. CIFS, NFS</p> <p>5.2. zapewniającym deduplikację na źródle, wymagane wsparcie dla aplikacji Commvault (co najmniej na poziomie Media Server a także Client Direct przy użyciu storage accelerator), Veeam Backup and Replication (co najmniej na poziomie Veeam Data Mover), NetWorker na poziomie klienta, rozwiązania stworzone w oparciu o FUSE nie będą brane pod uwagę</p> <p>5.3. VTL (min. 10 jednocześnie)</p>
6.	Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, deduplikacja na źródle, VTL do oferowanej pojemności urządzenia
7.	Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: NFS co najmniej 10 TB/h (dane podawane przez producenta) oraz co najmniej 20 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta).
8.	<p>8.1. Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni, w tym jednocześnie:</p> <p>8.2. zapis danych minimum 150 strumieniami</p> <p>8.3. odczyt danych minimum 50 strumieniami</p> <p>8.4. replikacja minimum 50 strumieniami pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.</p>

	<p>8.5. Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.</p> <p>8.6. Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.</p>
9.	<p>Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych:</p> <p>9.1. StorageTek L180</p> <p>9.2. IBM TS 3500</p>
10.	Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7
11.	Urządzenie musi umożliwiać (w przypadku VTL'a) emulację minimum 250 napędów, emulację min. 30 000 slotów w przypadku poj. biblioteki taśmowej oraz emulację sumarycznie min. 60 000 slotów.
12.	Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.
13.	<p>13.1. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o wielkości nie większej niż 12 kB.</p> <p>13.2. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości.</p>
14.	Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A”, nie może zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki „B” w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych.
15.	<p>Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.</p> <p>Wymaganie nie będzie spełnione jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup'ową. Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych interfejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć</p>

	od konkretnej aplikacji backup'owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiegokolwiek aplikacji backup'owej również muszą być deduplikowane w sposób in-line
16.	Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line)
17.	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
18.	Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymagane dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych.
19.	<p>19.1. Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Commvault, Veeam Backup and Replication, NetWorker.</p> <p>19.2. W przypadku współpracy z każdą z poniższych aplikacji:</p> <p>19.2.1. Commvault</p> <p>19.2.2. Veeam Backup and Replication</p> <p>19.2.3. NetWorker</p> <p>urządzenie musi umożliwiać deduplikację na źródle (w przypadku Commvault: co najmniej na poziomie Media Server a także Client Direct przy użyciu storage accelerator, w przypadku Veeam Backup and Replication co najmniej na poziomie Veeam Data Mover), w przypadku NetWorker na poziomie klienta) i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.</p> <p>19.3. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby do oferowanego urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu.</p>
20.	<p>20.1. W przypadku przyjmowania backupów z Commvault, Veeam Backup and Replication, NetWorker, urządzenie musi umożliwiać deduplikację na źródle (co najmniej na poziomie Media Server dla CommVault, Data Mover dla Veeam, klienta dla NetWorker) i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC.</p> <p>20.2. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby do oferowanego urządzenia były transmitowane poprzez sieć FC jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu.</p>
21.	Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych.
22.	Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów (Eth) wykorzystywanych przez aplikację backupową.
23.	Wymagane wsparcie dla backupów typu Virtual Synthetics w przypadku aplikacji Commvault, Veeam Backup and Replication oraz NetWorker.
24.	W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
25.	Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.

26.	<p>Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych:</p> <p>26.1. Windows</p> <p>26.2. Linux (RedHat, SuSE)</p>
27.	<p>27.1. Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów:</p> <p>27.1.1. jeden do jednego</p> <p>27.1.2. wiele do jednego</p> <p>27.1.3. jeden do wielu</p> <p>27.1.4. kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C).</p> <p>27.2. Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację jest przedmiotem postępowania.</p>
28.	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
29.	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
30.	<p>W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez: Commvault oraz NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:</p> <p>30.1. replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących</p> <p>30.2. replikacji podlegają tylko te fragmenty danych (na poziomie bloków używanych do deduplikacji), które nie znajdują się na docelowym urządzeniu</p> <p>30.3. replikacja zarządzana jest z poziomu wymaganej aplikacji</p> <p>30.4. aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji</p>
31.	Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnienia urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.
32.	Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji.
33.	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej.
34.	<p>34.1. Oferowane urządzenie musi pozwalać na realizację oraz przechowywanie SnapShot'ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot'u.</p>

	34.2. Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtworzenia backupów).
35.	Urządzenie musi pozwalać na przechowywanie minimum 500 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.
36.	Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia).
37.	Urządzenie musi mieć możliwość podziału na minimum 10 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 10 logicznych części pracujących równolegle z pełną wydajnością urządzenia.
38.	Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia.
39.	Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem: 39.1. CIFS 39.2. NFS 39.3. VTL deduplikacja na źródle
40.	40.1. Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku. 40.2. Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora): 40.2.1. Możliwość zdjęcia blokady przed upływem ważności danych 40.2.2. Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wymagane wsparcie norm SEC 17a-4(f) oraz ISO Standard 15489-1 w zakresie ochrony danych, wymagane oficjalne wsparcie wymaganej blokady przez aplikację Commvault, Veeam Backup and Replication oraz NetWorker – wymagane potwierdzenie na oficjalnych stronach w/w aplikacji backup'owych oraz producenta oferowanego deduplikatora 40.3. Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem. 40.4. Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady. W każdym przypadku wymagana również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności.
41.	Urządzenie musi mieć możliwość przechowywania danych niezmiennych: 41.1. Video

	41.2. Grafika 41.3. Nagrania dźwiękowe 41.4. Pliki pdf na udziałach CIFS/NFS.
42.	Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup'owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja musi być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności).
43.	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.
44.	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).
45.	Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora), wymagane potwierdzenie w ogólnodostępnej dokumentacji. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności)
46.	Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication.
47.	Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta).
48.	Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni.
49.	Urządzenie musi mieć możliwość zarządzania poprzez 49.1. Interfejs graficzny dostępny z przeglądarki internetowej 49.2. Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)
50.	Oprogramowanie do zarządzania musi rezydować na oferowanym urządzeniu deduplikacyjnym.
51.	Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade'ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem.
52.	Urządzenie musi być rozwiązaniem kompletnym, apłiancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway.
53.	Warunki gwarancji 53.1. Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat.

- 53.2.** Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24 godziny na dobę przez 7 dni w tygodniu następującymi kanałami: telefonicznie i przez Internet.
- 53.3.** Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
- 53.4.** Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
- 53.5.** 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.
- 53.6.** Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
- 53.7.** Zamawiający oczekuje 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.
- 53.8.** Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
- 53.9.** Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
- 53.10.** 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.
- 53.11.** Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.
- 53.12.** 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.
- 53.13.** 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.

- 54.** Wymaga się wdrożenia urządzenia wraz z oprogramowaniem w infrastrukturze Zamawiającego, w zakresie:
- instalacji i konfiguracji urządzenia wraz z oprogramowaniem w infrastrukturze Zamawiającego,
 - instruktażu dla administratorów rozwiązania.