Nr postępowania: A-ZPI.272.2.11.2024.JM3 Załącznik nr 1 do SWZ

Postępowanie o udzielenie zamówienia publicznego prowadzone w trybie podstawowym o jakim stanowi art. 275 pkt 2 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r., poz. 1320 t.j.) na dostawę pn.:
„Podniesienie poziomu cyberbezpieczeństwa w Starostwie Powiatowym w Jarocinie”

OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI I – VIII

CZĘŚĆ I – SYSTEM KOPII BEZPIECZEŃSTWA

1. Kompleksowy system wykonywania kopii bezpieczeństwa środowiska informatycznego wraz z replikacją na nośniki taśmowe.

1.1. Oprogramowanie do backupu serwerów fizycznych i wirtualnych, stacji roboczych i ich replikacji na taśmy. Rozbudowa posiadanej przez Zamawiającego licencji Veeam Backup Essentials Universal / Veeam Data Platform Essentials Universal Subscription License Includes Enterprise Plus Edition features 5 instancji do wersji obsługującej ochronę 30 serwerów fizycznych oraz 80 szt. stacji roboczych wraz z obsługą replikacji na biblioteki taśmowe. Zamawiający dopuszcza ze względów licencyjnych uruchomienie dwóch odrębnych środowisk backupowych – do ochrony serwerów oraz stacji roboczych. Okres subskrypcji i wsparcia technicznego – 24 miesiące.

W przypadku dostawy oprogramowania równoważnego musi ono spełnić następujące minimalne wymagania podane poniżej:

a) Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie: minimalna liczba referencji 150, minimalna ocena z referencji 4,5,
b) Oprogramowanie musi wspierać minimum następujące systemy operacyjne jako źródła backupu: Microsoft Windows Server 2022, Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012, Microsoft Windows 11 (wersje 21H2, 22H2), Microsoft Windows 10 (wersje od 1909 do 22H2), Microsoft Windows 10 LTS (wersje LTSB 1607, LTSC 1809, LTSC 2021), CentOS 7.x, Debian 10.0 do 12.21, Oracle Linux 7 (UEK3) do 9 (UEK R7), Oracle Linux 7 do 9 (RHCK), RHEL 7.0 do 9.31, SLES 12 SP4 lub późniejszy, 15 SP1 lub późniejszy, Ubuntu: 18.04 LTS, 20.04 LTS, i 22.04 LTS,
c) Oprogramowanie musi wspierać następujące aplikacje i bazy danych jako źródła backupu: Microsoft Active Directory Microsoft Windows Server 2022 Microsoft Windows Server 2019 Microsoft Windows Server 2016, Microsoft SQL Server Microsoft SQL Server 2022 (środowsko Windows) Microsoft SQL Server 2019 (środowisko Windows) Microsoft SQL Server 2017 (środowisko Windows) Microsoft SQL Server 2016 SP2, PostgreSQL 16, PostgreSQL 15, PostgreSQL 14, PostgreSQL 13, PostgreSQL 12. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. Oprogramowanie musi zapewniać backup maszyn wirtualnych Windows oraz Linux zainstalowanych na platformie wirtualizacyjnej XCP-NG z wykorzystaniem zainstalowanego agenta. Oprogramowanie musi wspierać pełne odtworzenie backupowanego środowiska na podstawie dedykowanego nośnika uruchomieniowego – tzw. Disaster Recovery,
d) Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków. Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: pełny, pełny syntetyczny,

przyrostowy i odwrotnie przyrostowy (tzw. reverse-incremental). Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym. Oprogramowanie musi oferować funkcjonalność, umożliwiającą samodzielne odtwarzanie użytkownikom plików. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.,

e) Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych i systemach operacyjnych. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Oprogramowanie musi oferować ten mechanizm z dokładnością do datastoru. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Oprogramowanie musi wspierać kopiowanie backupów na taśmy. Oprogramowanie musi posiadać wsparcie dla protokołu NDMP (Network Data Management Protocol). Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son). Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji z wykorzystaniem wbudowanej akceleracji WAN. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik. Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta końcowego. Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs, BSD: UFS, UFS2, Solaris: ZFS, UFS, Mac: HFS, HFS+, Windows: NTFS, FAT, FAT32, ReFS, Novell OES, NSS. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. Oprogramowanie musi wspierać odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Oprogramowanie musi

wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. Oprogramowanie musi pozwalać na zaprezentowanie baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego. Oprogramowanie musi wspierać także metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.,

f) Wdrożenie dostarczonego równoważnego oprogramowania. Zamawiający wymaga aby dostarczone oprogramowanie zostało zainstalowane i skonfigurowane wraz z wdrożeniem polityk backupowych w środowisku Zamawiającego przez zespół Wykonawcy stacjonarnie w siedzibie Zamawiającego. Obejmuje to: zaprojektowanie w współpracy z Zamawiającym harmonogramu wykonywania kopii, z uwzględnieniem środowiska Zamawiającego, instalację oprogramowania w środowisku Zamawiającego. implementację harmonogramu wykonywania kopii w zainstalowanym oprogramowaniu, wykonanie testowych kopii środowiska Zamawiającego wraz z weryfikacją poprawności ich wykonania. Testy odtworzenia danych środowiska Zamawiającego zarówno pojedynczych plików, aplikacji jak i kompletnych serwerów i stacji roboczych.,
g) Przygotowanie i przekazanie Zamawiającemu dokumentacji powykonawczej.,
h) Warsztaty z obsługi oprogramowania. Zamawiający wymaga aby warsztaty z zakresu instalacji, konfiguracji i obsługi oprogramowania zrealizowane były przez ośrodek posiadający autoryzację producenta oprogramowania i przeprowadzone były dla 2 administratorów Zamawiającego, trwały co najmniej 28 h (7 dni x 4 h) w tym wykłady i warsztaty praktyczne, zawierały omówienie funkcji oprogramowania, metod wdrożenia, konfiguracji i czynności administracyjnych, wydany był certyfikat lub zaświadczenie wystawione przez ośrodek szkoleniowy, świadczące o ukończeniu szkolenia. Zamawiający wymaga aby warsztaty przeprowadzone były w trybie stacjonarnym w siedzibie Zamawiającego na sprzęcie Wykonawcy. Warsztaty muszą się odbyć w maksymalnym terminie 2 tygodni liczonym od dnia podpisania protokołu odbioru wdrożenia systemu backupu.,
i) Wsparcie techniczne. Wykonawca zobowiązuje się do świadczenia usług wsparcia technicznego w okresie 24 miesięcy licząc od dnia podpisania protokołu odbioru na następujących warunkach: czas reakcji w przypadku krytycznego błędu (awarii) oprogramowania, gdy system o znaczeniu krytycznym dla Zamawiającego jest niedostępny lub nie działa – będzie nie dłuższy niż 2 godziny od momentu zgłoszenia, czas reakcji w przypadku bardzo poważnego błędu (awarii) oprogramowania, gdy system o znaczeniu produkcyjnym dla Zamawiającego jest dostępny w ograniczonym zakresie – będzie nie dłuższy niż 8 godzin od momentu zgłoszenia. W okresie trwania wsparcia technicznego Wykonawca zapewni Zamawiającemu dostęp do nowych wersji oprogramowania. Przyjmowanie zgłoszeń serwisowych i liczenie czasu reakcji realizowane będzie w godzinach od 7:00 do 16:00 w dni robocze, od poniedziałku do piątku.

1.2. System operacyjny Windows Server 2022 Standard 64 bit PL lub równoważny, licencja dla 16 rdzeni do obsługi oprogramowania do backupu z punktu 1.1. Liczba licencji – 1 szt. W przypadku systemu operacyjnego równoważnego musi on umożliwiać instalację oprogramowania z punktu 1.1 oraz wspierać wszystkie jego funkcjonalności wymienionej poniżej.

1. Współpraca z procesorami o architekturze x86 – 64bit.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 2 procesory oraz 16 rdzeni.

5. Praca w roli klienta domeny Microsoft Active Directory.
6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016.
7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
11. Możliwość uruchomienia roli serwera stron WWW.
    1. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
    2. Możliwość wykorzystania standardu http/2.
12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
18. Wbudowany mechanizm podłączania zasobów poprzez protokół iSCSI,
19. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,
20. Wbudowane szyfrowanie dysków przy pomocy wbudowanych w system narzędzi;
    1. Dostępne metody odblokowania woluminu:
        1. Automatycznie na podstawie danych z moduł TPM
        2. Za pomocą nośnika wymiennego
        3. Wprowadzając kod PIN
        4. Wprowadzając hasło
    2. Możliwość awaryjnego odblokowania za pomocą kodu odzyskiwania.
21. Możliwość uruchamiania aplikacji wykorzystujących technologię ASP.NET, Java, .NET Framework, .NET Core
22. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
23. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
24. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.

25. Mechanizmy logowania w oparciu o:
    1. login i hasło,
    2. karty z certyfikatami (smartcard),
26. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
    1. określonych grup użytkowników,
    2. zastosowanej klasyfikacji danych,
    3. centralnych polityk dostępu w sieci,
    4. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
27. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
28. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
29. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
30. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
    2. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        1. podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        2. ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        3. odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
        4. bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.,
    3. zdalna dystrybucja oprogramowania na stacje robocze,
    4. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,
    5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        1. Dystrybucję certyfikatów poprzez http,
        2. Konsolidację CA dla wielu lasów domeny,
        3. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
        4. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
    6. szyfrowanie plików i folderów,
    7. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
    8. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
    9. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
    10. wsparcie dla protokołu IP w wersji 6 (IPv6),
    11. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
    12. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera).

13. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
14. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
15. mechanizmy wirtualizacji mające wsparcie dla
    1. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
    2. obsługi ramek typu jumbo frames dla maszyn wirtualnych
    3. obsługi 4-KB sektorów dysków,
    4. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
    5. możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
16. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
17. wsparcie dla rozwiązania Kubernetes.
18. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
19. mechanizmy deduplikacji i kompresji na wolumenach.
20. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty
21. mechanizm konfiguracji połączenia VPN do platformy Azure.
22. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu
23. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów
24. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).

CZĘŚĆ II – URZĄDZENIA PAMIĘCI MASOWEJ

1. Urządzenia pamięci masowej.

1.1. Macierz ujednolicona (plikowa-blokowa) wyposażona w dwa kontrolery – 1 szt.

Minimalne parametry	
Obudowa	Do instalacji w standardowej szafie RACK 19” z kompletem szyn przesuwnych. Macierz musi zajmować wysokość maksymalnie 2U i pozwalać na instalacje min. 12 dysków.
Możliwości rozbudowy	Do minimum 440 dysków poprzez podłączenie jednostek rozszerzających w różnych wersjach, minimum: • 12-zatokowa na dyski 2.5”/3.5 w obudowie RACK 2U, • 16-zatokowa na dyski 2.5”/3.5 w obudowie RACK 3U, • 24-zatokowa na dyski 2.5”/3.5 w obudowie RACK 4U, • 24-zatokowa na dyski 2.5” w obudowie RACK 2U.
Obsługiwane dyski	Minimum: • 2.5" 12Gb/s SAS SSD, • 2.5" 12Gb/s SAS 10,000 RPM HDD, • 3.5" 12Gb/s NL-SAS 7,200 RPM HDD. Macierz musi umożliwiać zastosowanie dysków rożnych producentów bez ograniczenia do dysków tego samego producenta co macierz (brak tzw. „vendor lock”).
Zainstalowane dyski	Minimum 12 dysków zgodnych z listą kompatybilności oferowanej macierzy oraz

	charakteryzujących się następującymi parametrami: • pojemność: minimum 8TB, • interfejs: o przepustowości min. 12Gb/s, • dopuszczalna temperatura otoczenia podczas pracy: od 5°C do 60°C, • odporność na wstrząsy w stanie spoczynku (2 ms, G): minimum 250s, • MTBF: minimum 2 miliony, • gwarancja: minimum 60 miesięcy. Możliwość zgłoszenia dysku w przypadku awarii z opcją pozostawienia uszkodzonego nośnika u Zamawiającego.
Kontrolery	Dwa sprzętowe kontrolery pracujące w trybie active-active.
Cache kontrolera	Minimum 8GB z korekcją błędów z możliwością rozbudowy do minimum 192GB.
Wentylatory	Wentylatory lub moduły wentylatora z możliwością wymiany podczas pracy macierzy.
Zasilanie	Redundantny zasilacz o mocy minimalnej pozwalającej na bezproblemową pracę macierzy w przypadku awarii jednego modułu zasilacza o certyfikacie sprawności 80 PLUS Platinum lub wyższym.
Obsługiwane typy RAID	Minimum RAID 0, 1, 5, 6, 10, 50, 60
Interfejsy kontrolera	Minimum: • 1 port 1GbE RJ-45 LAN (zarządzanie), • 2 porty o przepustowości 12Gb/s (do podłączania jednostek rozszerzających), • 4 porty 10GbE SFP+ iSCSI (z kompletem modułów 10Gb/s SFP+ SR).
Rozbudowa interfejsów kontrolera	Możliwość zamontowania dodatkowych kart rozszerzeń w celu uzyskania minimum 10 portów 10GbE SFP+ na kontroler. Nie zezwala się na oferowanie rozwiązania, które do uzyskania wymaganej ilości portów komunikacyjnych będzie wymagało wymiany zainstalowanych wcześniej lub będących wyposażeniem fabrycznym kart sieciowych.
Oprogramowanie i funkcjonalności	Wymagane funkcjonalności: – Migawki (minimalnie 4096 migawek na cały system), – Thin provisioning z odzyskiwaniem miejsca, – Zdalna replikacja w trybie asynchronicznym, – Konfiguracja Quality of Service (QoS), – Automatyczne warstwowanie danych, – Pamięć podręczna SSD Cache, – Obsługa LACP, Multi-pathing, Trunking oraz Jumbo frame, – Wsparcie dla RESTful API. Funkcjonalności dostępne po zakupie dodatkowej licencji: – Zdalna replikacja w trybie synchronicznym. Nie jest wymagane dostarczenie licencji na etapie dostawy macierzy. Wymagana jest możliwość zakupu takiej licencji osobno po zakupie macierzy.
Obsługiwane protokoły	Minimum CIFS, NFS, iSCSI.
Wsparcie dla systemów operacyjnych	Minimum Windows Server 2022
Certyfikaty	Minimum CE i FCC. Macierz musi być wyprodukowana zgodnie z normą ISO 9001:2015 i ISO 14001:2015.
Dokumentacja	Wykonawca przekaże Zamawiającemu w dniu dostawy niezbędną dokumentację w języku polskim lub angielskim.

Deklaracje	Oferowane urządzenia posiadają deklarację zgodności CE.
Gwarancja	Minimum 60 miesięcy gwarancji producenta na dyski. Minimum 60 miesięcy gwarancji w tym 36 miesięcy gwarancji Next Business Day producenta na macierz. W przypadku potwierdzonej awarii sprzętowej macierzy dostarczone zostaną sprawne, pojedyncze elementy macierzy (np. moduł zasilacza, kontroler). Wymagana jest możliwość sprawdzenia typu i ważności gwarancji, a także szczegółowej konfiguracji sprzętowej poprzez dedykowaną stronę producenta. Strona ta po podaniu unikalnego numeru identyfikacyjnego macierzy powinna udostępniać informacje dotyczące modelu macierzy, wersji oprogramowania, zamontowanych dodatkowych kart rozszerzeń, pamięci RAM, aktywowanych licencji oraz modelu i wersji oprogramowania zainstalowanych dysków HDD i SSD.
Inne	Dostarczony sprzęt musi być fabrycznie nowy, nie używany w innych środowiskach ani projektach, sprawny technicznie, kompletny, gotowy do pracy, wyprodukowany nie wcześniej niż 12 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Zamawiający zastrzega sobie prawo, aby Wykonawca na etapie dostawy na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży. Wraz z macierzą wszystkie niezbędne kable połączeniowe.

1.2. Zewnętrzna pamięć masowa z interfejsem SAS kompatybilna z urządzeniem z Części II, punktu 1.1. niniejszej specyfikacji wraz z niezbędnymi kontrolerami do podłączenia. Jednostka rozszerzająca wyposażona w dwa kontrolery do macierzy ujednoliconej. Liczba sztuk – 2.

Minimalne parametry	
Obudowa	Do instalacji w standardowej szafie RACK 19” z kompletem szyn przesuwnych. Macierz musi zajmować wysokość maksymalnie 2U i pozwalać na instalacje min. 12 dysków.
Obsługiwane dyski	Minimum: • 2.5" 12Gb/s SAS SSD, • 2.5" 12Gb/s SAS 10,000 RPM HDD, • 3.5" 12Gb/s NL-SAS 7,200 RPM HDD. Jednostka musi umożliwiać zastosowanie dysków rożnych producentów bez ograniczenia do dysków tego samego producenta co macierz (brak tzw. „vendor lock”).
Zainstalowane dyski	Minimum 12 dysków zgodnych z listą kompatybilności oferowanej macierzy oraz charakteryzujących się następującymi parametrami: • pojemność: minimum 8TB, • interfejs: o przepustowości min. 12Gb/s, • dopuszczalna temperatura otoczenia podczas pracy: od 5°C do 60°C, • odporność na wstrząsy w stanie spoczynku (2 ms, G): minimum 250s, • MTBF: minimum 2 miliony, • gwarancja: minimum 60 miesięcy. Możliwość zgłoszenia dysku w przypadku awarii z opcją pozostawienia uszkodzonego nośnika u Zamawiającego.

Kontrolery	Dwa sprzętowe kontrolery pracujące w trybie active-active.
Wentylatory	Wentylatory lub moduły wentylatora z możliwością wymiany podczas pracy macierzy.
Zasilanie	Redundantny zasilacz o mocy minimalnej pozwalającej na bezproblemową pracę macierzy w przypadku awarii jednego modułu zasilacza o certyfikacie sprawności 80 PLUS Platinum lub wyższym.
Interfejsy kontrolera	Minimum 2 porty o przepustowości 12Gb/s wraz z okablowaniem potrzebnym do prawidłowego połączenia z głównej macierzy z jednostką rozszerzającą z zastosowaniem minimum dwóch ścieżek (minimum jedna ścieżka na kontroler).
Certyfikaty	Minimum CE i FCC. Jednostka musi być wyprodukowana zgodnie z normą ISO 9001:2015 i ISO 14001:2015.
Dokumentacja	Wykonawca przekaże Zamawiającemu w dniu dostawy niezbędną dokumentację w języku polskim lub angielskim.
Gwarancja	Minimum 60 miesięcy gwarancji producenta na dyski. Minimum 36 miesięcy gwarancji Next Business Day producenta macierzy. W przypadku potwierdzonej awarii sprzętowej dostarczone zostaną sprawne, pojedyncze elementy macierzy (np. moduł zasilacza, kontroler). Nie dotyczy dysków. Wymagana jest możliwość sprawdzenia typu i ważności gwarancji, a także szczegółowej konfiguracji sprzętowej poprzez dedykowaną stronę producenta. Strona ta po podaniu unikalnego numeru identyfikacyjnego macierzy powinna udostępniać informacje dotyczące modelu macierzy, wersji oprogramowania, zamontowanych dodatkowych kart rozszerzeń, pamięci RAM, aktywowanych licencji oraz modelu i wersji oprogramowania zainstalowanych dysków HDD i SSD.
Inne	Dostarczony sprzęt musi być fabrycznie nowy, nie używany w innych środowiskach ani projektach, sprawny technicznie, kompletny, gotowy do pracy, wyprodukowany nie wcześniej niż 12 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Zamawiający zastrzega sobie prawo, aby Wykonawca na etapie dostawy na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży. Wraz z zewnętrzną pamięcią masową wszystkie niezbędne kable połączeniowe.
Deklaracje	Oferowane urządzenia posiadają deklarację zgodności CE.

CZEŚĆ III – BIBLIOTEKA TAŚMOWA

1. Biblioteka taśmowa LTO9 wraz z kartą kontrolera oraz nośnikami LTO9 – 1 szt.

Minimalne parametry	
Rodzaj obudowy	2U 19” RACK
Liczba slotów na taśmy LTO	24 szt.
Liczba magazynków	2 szt.
Slot wymiany nośników / czytnik kodów kreskowych	Tak
Liczba napędów taśmowych LTO HH	2 szt.
Liczba zasilaczy	1 szt.
Panel do zarządzania urządzeniem	Wbudowany interaktywny panel sterowania LCD
Zdalne zarządzanie	Dedykowany interfejs Ethernet RJ 45. Wielojęzyczny
Niezawodność	100.000 h (MTBF = Mean Time Between Failure)

Zainstalowany napęd LTO HH	LTO-9 18TB /45TB – pojemność natywna/z kompresją – 1 szt.
Interfejs biblioteki	2 porty o przepustowości 12 Gb/s
Karta kontrolera do serwera	Typ: SAS/SATA HBA. Interfejs PCIe 3.0 x 8, liczba portów miniSAS 12 Gb/s mSAS SFF-8644– 2 szt., format karty LOW PROFILE, kompatybilna z oferowaną biblioteką i serwerem Dell R730XD z dwoma portami o przepustowości 12Gb/s umożliwiający podłączenie się do biblioteki taśmowej – 1 szt.
Akcesoria	Kabel połączeniowy o długości 2m. Szyny montażowe RACK dedykowane do urządzenia, nośnik LTO 9 – 28 sztuk.
Wsparcie techniczne/Gwarancja	36 miesięcy gwarancji producenta na urządzenie. Serwis urządzeń realizowany przez producenta lub autoryzowanego partnera serwisowego producenta lub dystrybutora sprzętu. 3 lata serwisu szybkiej wymiany komponentów.
Inne	Dostarczony sprzęt musi być fabrycznie nowy, nie używany w innych środowiskach ani projektach, sprawny technicznie, kompletny, gotowy do pracy, wyprodukowany nie wcześniej niż 12 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Zamawiający zastrzega sobie prawo, aby Wykonawca na etapie dostawy na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.
Deklaracje	Oferowane urządzenia posiadają deklarację zgodności CE.

CZĘŚĆ IV – SPRZĘT KOMPUTEROWY I SIECIOWY

1. Zasilacze awaryjne UPS do serwerów i macierzy dyskowych oraz biblioteki taśmowej – 4 szt.

Minimalne parametry	
Rodzaj obudowy	Montowana do szafy RACK 19”
Architektura zasilacza	online
Moc skuteczna	3000W
Czas podtrzymania dla obciążenia 50%	10 minut
Kształt napięcia wyjściowego	Sinusoidalny – pełna sinusoida
Zimny start	Tak
Przyłącza wyjściowe	8 szt.
Panel do zarządzania urządzeniem	Wbudowany panel sterowania LCD. Wyświetlanie predykcji czasu podtrzymania na baterii.
Możliwość podłączenia modułów bateryjnych	Tak
Akcesoria	Kabel zasilający do urządzenia. Szyny montażowe RACK dedykowane do urządzenia.

Wsparcie techniczne/Gwarancja	36 miesięcy gwarancji producenta na urządzenie. Serwis urządzeń realizowany przez producenta lub autoryzowanego partnera serwisowego producenta lub dystrybutora sprzętu.
Inne	Dostarczony sprzęt musi być fabrycznie nowy, nie używany w innych środowiskach ani projektach, sprawny technicznie, kompletny, gotowy do pracy, wyprodukowany nie wcześniej niż 12 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Zamawiający zastrzega sobie prawo, aby Wykonawca na etapie dostawy na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.
Deklaracje	Oferowane urządzenia posiadają deklarację zgodności CE.

2. Przełącznik sieciowy światłowodowy klasy Enterprise – 2 szt.

Minimalne parametry	
Obudowa	Obudowa typu rack o wysokości 1U
Typ, prędkość i liczba portów	28 portów SFP+ 10 Gb/s
Typ, prędkość i liczba portów	4 porty 25 Gb/s SFP28
Przepustowość przełączania	760 Gbps
Panel do monitorowania urządzeniem	Ekran dotykowy LCD
Zasilanie	Wbudowany zasilacz 1 szt., opcja redundancji zasilania
Zarządzanie urządzeniem	Zarządzanie urządzeniem poprzez posiadany przez Zamawiającego kontroler sprzętowy Ubiquiti UDM SE
Akcesoria	Kabel zasilający do urządzenia. Zestaw do montażu w szafie RACK dedykowany do urządzenia.
Wsparcie techniczne/Gwarancja	12 miesięcy gwarancji producenta na urządzenie. Serwis urządzeń realizowany przez producenta lub autoryzowanego partnera serwisowego producenta lub dystrybutora sprzętu.
Inne	Dostarczony sprzęt musi być fabrycznie nowy, nie używany w innych środowiskach ani projektach, sprawny technicznie, kompletny, gotowy do pracy, wyprodukowany nie wcześniej niż 12 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Zamawiający zastrzega sobie prawo, aby Wykonawca na etapie dostawy na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.
Deklaracje	Oferowane urządzenia posiadają deklarację zgodności CE.

3. Dysk twardy – 4 szt.

Minimalne parametry	
Dysk twardy	Dysk twardy typu SSD o wielkości 2,5 cala dedykowany do pracy w serwerach lub urządzeniach typu NAS w obudowie typu hot-plug. Pojemność 7,68TB, format 2.5", interfejs SATA, prędkość odczytu minimalna 560MBs MB/s, prędkość zapisu minimalna

	530MB/s, odczyt losowy 94,000 IOPS, zapis losowy 34,000 IOPS, rodzaj kości pamięci 3D TLC, niezawodność MTBF 2 000 000 godz. Dysk ma być w pełni zgodny parametrami z posiadanymi przez Zamawiającego dyskami Kingston DC600M 7680GB 2,5" SATA (SEDC600M7680G i zapewniać bezproblemowe działanie w macierzy typu RAID utworzoną z tych dysków, działającą w środowisku Zamawiającego.
Gwarancja i wsparcie techniczne oraz serwis	60 miesięcy gwarancji producenta lub dostawcy. Wymiana dysku na nowy w ciągu 72 godzin od zgłoszenia.
Inne	Dostarczony sprzęt musi być fabrycznie nowy, nie używany w innych środowiskach ani projektach, sprawny technicznie, kompletny, gotowy do pracy, wyprodukowany nie wcześniej niż 24 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Zamawiający zastrzega sobie prawo, aby Wykonawca na etapie dostawy na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.
Deklaracje	Oferowane urządzenia posiadają deklarację zgodności CE.

4. Dysk twardy – 30 szt.

Minimalne parametry	
Dysk twardy	Dysk twardy typu SAS dedykowany do pracy w serwerach, urządzeniach pamięci masowej i centrach danych. Pojemność 8 TB, format 3.5 cala, interfejs SAS 12 Gbit/s, pamięć podręczna 256 MB, prędkość obrotowa 7200RPM, MTBF 2 000 000 godz.
Gwarancja i wsparcie techniczne oraz serwis	60 miesięcy gwarancji producenta lub dostawcy. Wymiana dysku na nowy w ciągu 72 godzin od zgłoszenia.
Inne	Dostarczony sprzęt musi być fabrycznie nowy, nie używany w innych środowiskach ani projektach, sprawny technicznie, kompletny, gotowy do pracy, wyprodukowany nie wcześniej niż 24 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Zamawiający zastrzega sobie prawo, aby Wykonawca na etapie dostawy na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.
Deklaracje	Oferowane urządzenia posiadają deklarację zgodności CE.

5. Zasilacze awaryjne UPS dla stacji roboczych – 35 szt.

Minimalne parametry	
Moc skuteczna	300W
Czas przełączania	maks. 10 ms. typowo max. 8 ms.
Czas podtrzymania dla obciążenia 50%	min. 13 minut
Kształt napięcia wyjściowego	Sinusoida modyfikowana lub Pełna sinusoida
Architektura	Offline lub Line-interactive lub on-line
Gniazdo zasilania	co najmniej 3 gniazda typ Typ E lub typ F lub typ C14
Panel informacyjny na urządzeniu	Informacja o pracy z sieci, z baterii, przeciążeniu i konieczności wymiany baterii. Urządzenie sprawdza czy bateria wymaga wymiany poprzez cykliczne

	wykonywanie testu akumulatora. Do przeprowadzenia testu nie jest wymagane oprogramowania zainstalowane na stacji roboczej.
Bezpiecznik	Automatyczny
Wymiana akumulatora	Przez użytkownika końcowego. Beznarzędziowa.
Komunikacja	Urządzenie wyposażone w złącze USB i przewód USB. Zasilacz zapewniający pełną współpracę z systemami Windows 10 oraz Windows 11.

6. Przełącznik sieciowy 2,5 gigabitowy klasy Enterprise – 3 szt.

Minimalne parametry	
Obudowa	Obudowa typu rack o wysokości 1U
Typ, prędkość i liczba portów Ethernet	48 portów RJ45 2.5 Gb/s. Każdy z portów wspierający zasilanie POE/POE+
Typ, prędkość i liczba portów SFP	4 porty SFP+ z możliwością pracy mieszanej 1 lub 10 Gb/s
Przepustowość przełączania	320 Gbps
Funkcje warstwy 2	IGMP snooping, RSTP, loop protection, izolacja portów, voice VLAN, port mirroring, LACP, 802.1x, jumbo frames, DHCP snooping, izolacja DHCP
Funkcje warstwy 3	DHCP relay, routing pomiędzy VLAN
Panel do monitorowania urządzeniem	Ekran dotykowy LCD
Zasilanie	Wbudowany zasilacz 1 szt. ,opcja redundancji zasilania
Zarządzanie urządzeniem	Zarządzanie urządzeniem poprzez posiadany przez Zamawiającego kontroler sprzętowy Ubiquiti UDM SE
Akcesoria	Kabel zasilający do urządzenia. Zestaw do montażu w szafie RACK dedykowany do urządzenia.
Wsparcie techniczne/ Gwarancja	12 miesięcy gwarancji producenta na urządzenie. Serwis urządzeń realizowany przez producenta lub autoryzowanego partnera serwisowego producenta lub dystrybutora sprzętu.
Inne	Dostarczony sprzęt musi być fabrycznie nowy, nie używany w innych środowiskach ani projektach, sprawny technicznie, kompletny, gotowy do pracy, wyprodukowany nie wcześniej niż 12 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Zamawiający zastrzega sobie prawo, aby Wykonawca na etapie dostawy na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.
Deklaracje	Oferowane urządzenia posiadają deklarację zgodności CE.

7. Klucze sprzętowe do logowania – 6 szt.

Minimalne parametry	
Typ	Klucze sprzętowe gwarantujące bezpieczeństwo w Internecie chroniące przed ryzykiem wyłudzenia danych i przejęcia konta, pozwalający na łatwy dostęp do bezpiecznego logowania w serwisach internetowych.

Interfejs	USB typu C, NFC
Kryptografia	RSA 2048, RSA 4096 (PGP)
Protokoły zabezpieczające	FIDO/FIDO2, WebAuthn, U2F, Smart card, OATH – TOTP
Gwarancja	Minimum 12 miesięcy gwarancji.
Dołączone akcesoria	przejściówka umożliwiająca podłączenie klucza do złącza USB A

8. Bezprzewodowy punkt dostępowy – 5 szt.

Minimalne parametry	
Obudowa	Z możliwością montażu na ścianie lub suficie za pomocą dołączonych akcesoriów. Dioda LED informująca o zasilaniu urządzenia
Typ, prędkość i liczba portów Ethernet	1 port RJ45 2.5 Gb/s. wspierający zasilanie POE lub POE+
Typ sieci bezprzewodowej	802.11a/b/g/n/ac/ax/be (WiFi 6/6E, WiFi 7)
Szyfrowanie	WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3/PPSK)
Przepustowość sieci bezprzewodowej	2,4 GHz – 680 Mb/s 5GHz – 8,6 Gb/s 6GHz – 5,7 Gb/s
Zysk energetyczny	2,4 GHz – 4 dBi 5GHz – 6 dBi 6GHz – 5,9 dBi
Zarządzanie urządzeniem	Zarządzanie urządzeniem poprzez posiadany przez Zamawiającego kontroler sprzętowy Ubiquiti UDM SE
VLAN	802.1Q
Wsparcie techniczne/Gwarancja	12 miesięcy gwarancji producenta na urządzenie. Serwis urządzeń realizowany przez producenta lub autoryzowanego partnera serwisowego producenta lub dystrybutora sprzętu.
Inne	Dostarczony sprzęt musi być fabrycznie nowy, nie używany w innych środowiskach ani projektach, sprawny technicznie, kompletny, gotowy do pracy, wyprodukowany nie wcześniej niż 12 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Zamawiający zastrzega sobie prawo, aby Wykonawca na etapie dostawy na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.
Deklaracje	Oferowane urządzenia posiadają deklarację zgodności CE.

CZĘŚĆ V – OPROGRAMOWANIE DO OCHRONY INFRASTRUKTURY IT

1. Podniesienie poziomu wydajności oraz zabezpieczeń środowiska IT.

1.1. Oprogramowanie do wykrywania i reagowania Extended Detection & Response – XDR, służące do identyfikacji nietypowych zachowań i naruszeń bezpieczeństwa firmowej sieci – zestaw licencji na 100 stanowisk z subskrypcją na 2 lata

Migracja z posiadanej przez Zamawiającego aktywnej licencji ESET PROTECT Essential ON-PREM do wersji ESET PROTECT Elite – licencja na 100 stanowisk na 2 lata. Ważność posiadanej

obecnie licencji do 2026.06.30	
W przypadku dostawy oprogramowania równoważnego musi ono spełnić następujące poniższe wymagania:	
Parametry funkcjonalne	**Ochrona stacje robocze Linux:** 1. Rozwiązanie musi wspierać systemy operacyjne Ubuntu Desktop, Red Hat Enterprise Linux, SUSE Linux Enterprise Desktop oraz Linux Mint. 2. Rozwiązanie musi posiadać wsparcie dla dystrybucji 64-bitowych. 3. Pomoc (help) musi być dostępna co najmniej w języku polskim oraz angielskim. 4. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 5. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 6. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami. 7. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. 8. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 9. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. 10. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 11. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. 12. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie. 13. Rozwiązanie musi posiadać możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów. 14. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Administrator musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie. 15. Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 16. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 17. Aktualizacje silnika detekcji muszą być dostępne z Internetu, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP). 18. Rozwiązanie musi posiadać możliwość pobierania aktualizacji za pośrednictwem serwera proxy. 19. Rozwiązanie musi być wyposażone tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 20. Wsparcie techniczne dla rozwiązania musi być świadczone w języku polskim przez

	polskiego dystrybutora autoryzowanego przez producenta programu. **Ochrona stacje robocze – macOS:** 1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) lub nowszych. 2. Rozwiązanie musi wspierać architekturę Apple Silicon (ARM). 3. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. 4. Pomoc w rozwiązaniu (help) musi być dostępna co najmniej w języku polskim oraz angielskim. 5. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 6. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 7. Rozwiązanie musi posiadać funkcjonalność, która w momencie wykrycia trybu pełnoekranowego ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań. 8. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. 9. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 10. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności). 11. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych. 12. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. 13. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 14. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. 15. Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 16. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie. 17. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie mają być wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. 18. Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 19. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego

	zagrożenia z katalogu kwarantanny do laboratorium producenta. 20. Rozwiązanie musi posiadać ochronę przed atakami typu „phishing”. 21. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 22. Aktualizacja silnika detekcji rozwiązania musi być dostępna z Internetu, lokalnego zasobu sieciowego lub przy pomocy serwera HTTP. 23. Rozwiązanie musi posiadać możliwość pobierania aktualizacji za pośrednictwem serwera proxy. 24. Rozwiązanie musi umożliwiać automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego. 25. Rozwiązanie musi być wyposażone tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 26. Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji silnika detekcji i samego oprogramowania oraz dokonanym skanowaniu komputera. 27. Rozwiązanie musi umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień. 28. Rozwiązanie musi posiadać mechanizm Ochrony dostępu do stron internetowych monitoruje komunikację w ramach protokołu HTTP. 29. Rozwiązanie musi pozwalać na konfigurację portów, dla których ma się odbywać skanowanie protokołu HTTP. 30. Rozwiązanie musi posiadać możliwość zdalnego zarządzania z poziomu Administracji zdalnej. 31. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 32. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 33. Rozwiązanie musi umożliwiać definiowanie różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie. 34. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji w temacie zainfekowanej wiadomości o jej przeskanowaniu. 35. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 36. Wsparcie techniczne dla rozwiązania musi być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. **Ochrona stacje robocze – Windows:** 1. Rozwiązanie musi wspierać systemy Windows 10/Windows 11. 2. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows. 3. Rozwiązanie musi wspierać architekturę ARM64. 4. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. 5. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. 6. Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim. 7. Skuteczność rozwiązania potwierdzona nagrodami VB100 i AV-comparatives. 8. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami

	i innymi zagrożeniami. 9. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 10. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami. 11. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje. 12. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. 13. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie" lub według harmonogramu. 14. Rozwiązanie musi posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania. 15. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). 16. Rozwiązanie musi posiadać opcję skanowania „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 17. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu. 18. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych. 19. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. 20. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 21. Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku. 22. Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 23. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. 24. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera. 25. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. 26. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 27. Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 28. Rozwiązanie musi posiadać wbudowany konektor dla programu Microsoft Outlook. 29. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu Microsoft Outlook. 30. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta

	pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 31. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 32. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 33. Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie. 34. Rozwiązanie musi posiadać możliwość blokowania możliwości przeglądania wybranych stron internetowych. Rozwiązanie musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL. 35. Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora. 36. Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 37. Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 38. Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe. 39. Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta. 40. Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego. 41. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 42. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym. 43. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 44. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne. 45. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 46. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie. 47. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 48. Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika. 49. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek

	nowych zagrożeń mają być w pełni anonimowe. 50. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. 51. Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło. 52. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo. 53. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji. 54. Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. 55. Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń. 56. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. 57. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. 58. Rozwiązanie musi posiadać umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 59. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia. 60. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. 61. Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia. 62. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 63. W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 64. Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika. 65. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS). 66. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

	c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, d. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 67. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. 68. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. 69. Rozwiązanie musi posiadać zaawansowany skaner pamięci. 70. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych. 71. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 72. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 73. Rozwiązanie musi posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie. 74. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 75. Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera. 76. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji. 77. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. 78. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. 79. Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). 80. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 81. Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym. 82. W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania.

	83. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym. 84. Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń. 85. Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji. 86. Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline. 87. Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie. 88. W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji. 89. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej. 90. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia. 91. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny. 92. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. 93. Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki. 94. Rozwiązanie musi posiadać możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych. 95. Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji. 96. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie. 97. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 98. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia. 99. Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup. 100. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny. 101. Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść” 102. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. 103. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. 104. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. 105. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków,

	anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 106. Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet. 107. Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB. 108. Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. 109. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu. **Ochrona stacji roboczych – macOS:** 1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 10.12 lub nowszych. 2. Rozwiązanie musi wspierać architekturę Apple Silicon (ARM). 3. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. 4. Pomoc w rozwiązaniu (help) musi być dostępna co najmniej w języku polskim oraz angielskim. 5. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 6. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 7. Rozwiązanie musi posiadać funkcjonalność, która w momencie wykrycia trybu pełnoekranowego ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań. 8. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. 9. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 10. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności). 11. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych. 12. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. 13. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 14. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. 15. Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 16. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie. 17. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie mają być wysyłane automatycznie, oraz czy

	próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. 18. Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 19. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 20. Rozwiązanie musi posiadać ochronę przed atakami typu „phishing". 21. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych. Funkcja musi umożliwiać wyłączenie dostępu do nośników: płyta CD/DVD, pamięć masowa, karty sieciowe, drukarka USB, urządzenie do tworzenia obrazów, port szeregowy, urządzenie przenośne. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 22. Aktualizacja silnika detekcji rozwiązania musi być dostępna z Internetu, lokalnego zasobu sieciowego lub przy pomocy serwera HTTP. 23. Rozwiązanie musi posiadać możliwość pobierania aktualizacji za pośrednictwem serwera proxy. 24. Rozwiązanie musi umożliwiać automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego. 25. Rozwiązanie musi być wyposażone tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 26. Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji silnika detekcji i samego oprogramowania oraz dokonanym skanowaniu komputera. 27. Rozwiązanie musi umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień. 28. Rozwiązanie musi posiadać mechanizm Ochrony dostępu do stron internetowych monitoruje komunikację w ramach protokołu HTTP. 29. Rozwiązanie musi pozwalać na konfigurację portów, dla których ma się odbywać skanowanie protokołu HTTP. 30. Rozwiązanie musi umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy" na modyfikację konfiguracji programu. 31. Rozwiązanie musi posiadać możliwość zdalnego zarządzania z poziomu Administracji zdalnej. 32. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 33. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 34. Rozwiązanie musi umożliwiać definiowanie różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie. 35. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji w temacie zainfekowanej wiadomości o jej przeskanowaniu. 36. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.

	37. Wsparcie techniczne dla rozwiązania musi być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 38. Zapora osobista rozwiązania musi pracować w jednym z 2 trybów: a. Automatyczny z wyjątkami – umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł, b. Interaktywny – dla każdej nieznanej komunikacji generowane jest pytanie dla użytkownika o jej odblokowanie. 39. Rozwiązanie musi mieć możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego. 40. Rozwiązanie musi mieć możliwość odnotowania faktu nawiązania danego połączenia w dzienniku zdarzeń. 41. Rozwiązanie musi mieć możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu. 42. Rozwiązanie musi mieć możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla profilu: Publiczny, Praca, Dom. 43. Rozwiązanie musi oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. 44. Rozwiązanie musi mieć możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. 45. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. 46. Aktywacja stref ma się odbywać min. w oparciu o: interfejs sieciowy w systemie, sieć WiFi, podsieć IPv4/IPv6, zakres adresów IPv4/IPv6, Adres IPv4/IPv6. **Kontrola dostępu do stron internetowych:** 1. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli odwiedzanych stron internetowych. 2. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły. 3. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego. 4. Reguły mają być automatycznie aktywowane w zależności od zalogowanego użytkownika. 5. Rozwiązanie musi posiadać możliwość filtrowania URL w oparciu o co najmniej 140 kategorii i podkategorii. 6. Podstawowe kategorie w jakie rozwiązanie musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. 7. Lista adresów URL, znajdujących się w poszczególnych kategoriach, musi być na bieżąco aktualizowana przez producenta. 8. Użytkownik musi posiadać możliwość wyłączenia modułu kontroli dostępu do stron internetowych. **Ochrona stacje robocze – Windows:** 1. Rozwiązanie musi wspierać systemy Windows 10/Windows 11. 2. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.

	3. Rozwiązanie musi wspierać architekturę ARM64. 4. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim. 5. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. 6. Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim. 7. Skuteczność rozwiązania potwierdzona nagrodami VB100 i AV-comparatives. 8. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 9. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 10. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami. 11. Rozwiązanie musi integrować się z Intel Threat Detection Technology. 12. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje. 13. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików. 14. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu. 15. Rozwiązanie musi posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania. 16. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). 17. Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 18. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 19. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych. 20. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. 21. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 22. Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku. 23. Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 24. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. 25. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera. 26. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. 27. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 28. Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików

	i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 29. Rozwiązanie musi posiadać wbudowany konektor dla programu Microsoft Outlook. 30. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu Microsoft Outlook. 31. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 32. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 33. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 34. Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie. 35. Rozwiązanie musi posiadać możliwość blokowania możliwości przeglądania wybranych stron internetowych. Rozwiązanie musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL. 36. Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora. 37. Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 38. Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 39. Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe. 40. Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta. 41. Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego. 42. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 43. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym. 44. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. 45. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne. 46. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

	47. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie. 48. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 49. Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika. 50. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 51. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. 52. Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło. 53. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo. 54. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji. 55. Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. 56. Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń. 57. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. 58. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. 59. Rozwiązanie musi posiadać umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 60. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia. 61. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. 62. Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia. 63. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 64. W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 65. Administrator ma posiadać możliwość takiej konfiguracji rozwiązania,

	aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika. 66. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS). 67. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, d. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 68. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. 69. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. 70. Rozwiązanie musi posiadać zaawansowany skaner pamięci. 71. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych. 72. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 73. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 74. Rozwiązanie musi posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie. 75. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 76. Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera. 77. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji. 78. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. 79. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. 80. Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia

	(rollback). 81. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 82. Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym. 83. W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania. 84. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym. 85. Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń. 86. Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji. 87. Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline. 88. Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie. 89. W trakcie instalacji rozwiązanie ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM. 90. W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji. 91. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej. 92. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia. 93. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny. 94. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. 95. Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki. 96. Rozwiązanie musi posiadać możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych. 97. Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji. 98. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie. 99. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 100. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia. 101. Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed

	oprogramowaniem wymuszającym okup. 102. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny. 103. Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”. 104. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. 105. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. 106. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. 107. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 108. Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet. 109. Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB. 110. Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. 111. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu. **Ochrona przed spamem:** 1. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 2. Rozwiązanie musi umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. 3. Rozwiązanie musi umożliwiać automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. 4. Rozwiązanie musi posiadać możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego. 5. Rozwiązanie musi posiadać możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego. 6. Rozwiązanie musi posiadać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam. 7. Rozwiązanie musi możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam. 8. Rozwiązanie musi domyślnie współpracować z folderem „Wiadomości-śmieci”, dostępnym w programie Microsoft Outlook. 9. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana” 10. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana”. 11. Rozwiązanie musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera. **Zapora osobista (personal firewall):** 1. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: a. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, b. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, c. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący,

	zezwalając tylko na połączenia skonfigurowane przez administratora, d. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. 2. Rozwiązanie musi oceniać reguły zapory systemu Windows. 3. Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych. 4. Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie. 5. Rozwiązanie musi posiadać możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego. 6. Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj. 7. Rozwiązanie musi posiadać możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji. 8. Rozwiązanie musi posiadać możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet. 9. Rozwiązanie musi wykrywać modyfikację w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu. 10. Rozwiązanie musi posiadać możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. 11. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci. 12. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. 13. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie. 14. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6. 15. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci. 16. Rozwiązanie musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów: a. z aplikacją lokalną, którą administrator wskazuje z listy, b. z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP. **Kontrola dostępu do stron internetowych:** 1. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 2. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory. 3. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 4. Podstawowe kategorie, w jakie rozwiązanie musi być wyposażone to: materiały

	dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. 5. Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych. 6. Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta. 7. Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych. 8. Rozwiązanie musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj. 9. Rozwiązanie musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej. **Bezpieczna przeglądarka:** 1. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. 2. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 3. Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki. 4. Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę. 5. Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki. 6. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. **Ochrona urządzeń mobilnych opartych o system Android:** 1. Rozwiązanie musi wspierać system co najmniej Android 6.0. 2. Rozwiązanie musi wspierać rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa. 3. Rozwiązanie musi wspierać procesory: ARM z obsługą ARMv7 lub x86 Intel Atom. 4. Rozwiązanie musi posiadać ochronę plików w czasie rzeczywistym. 5. Rozwiązanie musi posiadać ochronę przed atakami typu „phishing”. 6. Rozwiązanie musi skanować wszystkie typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 7. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 8. Rozwiązanie musi posiadać ochronę proaktywną wykrywającą nieznane zagrożenia. 9. W przypadku wykrycia zagrożenia użytkownik musi otrzymać odpowiednie powiadomienie. 10. Rozwiązanie musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia. 11. Rozwiązanie musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). **Skanowanie na żądanie:**

	1. Rozwiązanie musi mieć możliwość skanowania zainstalowanych aplikacji. 2. Informacje o skanowaniu mają być przechowywane w plikach dziennika. 3. Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania. 4. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia. **Polityka ustawień:** 1. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej: a. połączenie Wi-Fi, b. GPS, c. usługi lokalizacyjne, d. pamięć, e. roaming danych, f. roaming połączeń, g. nieznane źródła, h. tryb debugowania, i. komunikacja NFC, j. szyfrowanie pamięci masowej, k. urządzenie zrootowane. **Kontrola aplikacji:** 1. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji. 2. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji. 3. Blokowanie aplikacji musi być możliwe w oparciu o: a. nazwę aplikacji, b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła. **Zabezpieczenia urządzenia:** 1. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej: a. minimalny poziom zabezpieczeń i złożoność blokady ekranu, b. maksymalną dopuszczaną liczbę błędnych prób odblokowania, c. odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie, d. czas, po którym automatycznie nastąpi blokada ekranu, e. ograniczenie dostępu do kamery wbudowanej w urządzenie. **Aktualizacje modułów:** 1. Rozwiązanie musi umożliwiać wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji. 2. Rozwiązanie musi mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje modułów co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin. 3. Rozwiązanie musi posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją. **Konfiguracja i zdalne zarządzanie:** 1. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu

	przeniesienia konfiguracji na inne urządzenie mobilne. 2. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją. **Szyfrowanie:** 1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 32-bit i 64-bit i Windows 11-64bit. 2. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku macOS 10.14 lub nowszej. 3. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). 4. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. 5. Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim. 6. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM. 7. Aplikacja musi mieć możliwość korzystania z technologii TCG OPAL – dyski sprzętowo szyfrowane. 8. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI. 9. W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania. 10. Aplikacja do szyfrowania musi być zarządzana z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej. 11. Konsola centralnego zarządzania musi pozwalać na wygenerowanie, dla każdej zaszyfrowanej stacji, dysku ratunkowego. 12. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej: a) ilość znaków, b) czy hasło ma zawierać wielkie litery, c) czy hasło ma zawierać małe litery, d) czy hasło ma zawierać cyfry, e) czy hasło ma zawierać znaki specjalne, f) okres ważności, g) ilość nieudanych logowań, h) możliwość zmiany hasła. 13. Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom. 14. Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku. **XDR (rozszerzone wykrywanie i reagowanie):** <u>Serwer</u> 1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych. 2. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL. 3. System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta. 4. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego

	czyszczenia bazy danych. 6. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta. 7. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 8. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. 9. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica". 10. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia. 11. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika. 12. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta. 13. Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne. 14. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej. 15. Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali. 16. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku. 17. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania. 18. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny. 19. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. 20. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych. 21. Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy. 22. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego

	oprogramowania firm trzecich. 23. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal). 24. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 25. Konsola administracyjna musi mieć możliwość tagowania obiektów. 26. Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli. 27. Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci. 28. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell. <u>Konektor</u> 1. Pełne wsparcie dla systemu Windows 10/ Windows 11 oraz Windows Server 2012/2012R2/2016/2019/2022. 2. Pełne wsparcie dla systemów macOS 10.15 i nowszych. 3. Pełne wsparcie dla systemów Linux RHEL 7.6+/RHEL 8/RHEL 9/Ubuntu 18.04/Ubuntu 20.04/Ubuntu 22.04/Debian 10/Debian 11/Debian 12 4. Wsparcie dla 32 i 64-bitowej wersji systemu Windows. 5. Konektor musi współpracować z produktem antywirusowym tego samego producenta. 6. Konektor nie może działać bez produktu antywirusowego tego samego producenta. 7. W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonane przez konektor. 8. Połączenie konektora do serwera zarządzającego musi być szyfrowane. 9. Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane. **Sandbox w chmurze:** 1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. 2. Rozwiązanie musi wykorzystywać do działania chmurę producenta. 3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. 6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. 7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. 8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. 9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. 10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. 11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.

	12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: a. czysty, b. podejrzany, c. bardzo podejrzany, d. szkodliwy. 13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. 14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. 15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia. **Ochrona serwera pocztowego – IBM Domino:** 1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych. 2. Rozwiązanie musi wspierać produkt IBM Domino w wersji 6.5.4 i nowsze oraz HCL Domino w wersji 11 i 12. 3. Rozwiązanie musi wspierać wiele instancji IBM Domino zainstalowanych na jednej fizycznej maszynie. 4. Rozwiązanie musi skanować pocztę na poziomie protokołu SMTP oraz NRPC. 5. Rozwiązanie musi umożliwiać skanowanie w środowiskach hybrydowych opartych na MS Office 365. 6. Rozwiązanie musi umożliwiać regularne skanowanie bazy poczty email przetrzymywanej w bazie danych Domino. 7. Rozwiązanie musi umożliwiać wskazanie zakresu czasowego wiadomości które mają być przeskanowane na żądanie w tym co najmniej wiadomości modyfikowane: a. w ciągu ostatniego miesiąca. b. w ciągu ostatniego tygodnia. c. w ciągu ostatnich 24 godzin. 8. Rozwiązanie musi wykrywać zagrożenia phishingowe podczas przesyłania zewnętrznej poczty, w przypadku bazy danych oraz w przypadku ochrony na żądanie. 9. Rozwiązanie musi umożliwiać wybór czynności wykonywanej w odniesieniu do wiadomości typu „phishing”: poddaj wiadomość kwarantannie, odrzuć wiadomość, porzuć wiadomość w trybie dyskretnym, brak czynności. 10. Rozwiązanie musi umożliwiać wybór czynności wykonywanej w odniesieniu do notatek typu „phishing”: przenieś notatkę do kosza, usuń wiadomość, wiadomość dotycząca kwarantanny, brak czynności. 11. Rozwiązanie musi umożliwiać tworzenie reguł dla przetwarzanej poczty w oparciu o: a. Temat wiadomości. b. Nadawcę wiadomości. c. Odbiorcy wiadomości. d. Nazwa bazy danych. e. Nazwa załącznika. f. Rozmiar załącznika. g. Typ załącznika. h. Wynik skanowania antyspamowego. i. Wynik skanowania antywirusowego. j. Zawierającego archiwum zabezpieczone hasłem.

	k. Zawierającego uszkodzone archiwum. 12. Rozwiązanie musi posiadać możliwość określenia akcji jaka zostanie wykonana w momencie gdy wiadomość zostanie przetworzona przez daną regułę w tym co najmniej: a. Poddania wiadomości kwarantannie. b. Usunięcia załącznika. c. Odrzucenia wiadomości z wysłaniem komunikatu do nadawcy. d. Cichego odrzucenia wiadomości. e. Wysłania powiadomienia. f. Pominięcia skanowania antyspamowego. g. Pominięcia skanowania antywirusowego. h. Przetworzenie przez pozostałe reguły. i. Zapisania informacji w plikach dziennika. 13. Rozwiązanie musi umożliwiać tworzenie reguł przy wykorzystaniu wbudowanego kreatora reguł. 14. Rozwiązanie musi umożliwiać automatyczne dodawanie dowolnego tagu do wiadomości potraktowanej jako SPAM. 15. Rozwiązanie musi umożliwiać dodawanie do wykluczeń ze skanowania wskazanych baz IBM Domino. 16. Rozwiązanie musi automatycznie tworzyć kwarantannę dla poczty na serwerze IBM Domino. 17. Rozwiązanie musi posiadać możliwość określenia ilości jednoczesnych wątków skanowania na żądanie. 18. Administrator musi mieć możliwość ustawienia zakresu czasowego po jakim z kwarantanny automatycznie będą usuwane najstarsze wiadomości. 19. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach firm trzecich. 20. Rozwiązanie musi być wyposażone w zaawansowany skaner pamięci chroniący przed skomplikowanymi zagrożeniami. 21. Rozwiązanie musi być wyposażona w mechanizm HIPS. 22. Mechanizm HIPS musi umożliwiać tworzenie własnych reguł przez Administratora w oparciu o: a. wpisy w rejestrze. b. Aplikacje. c. Pliki. 23. Rozwiązanie musi umożliwiać skonfigurowanie wyjątków ochrony przed atakami sieciowymi (IDS). 24. Rozwiązanie musi umożliwiać wykrywanie włamań wykorzystujących protokoły: SMB, RPC, RDP i informować użytkownika o wykryciu ataku. 25. Rozwiązanie musi wyświetlać powiadomienia po wykryciu ataku przechodzącego na luki zabezpieczeń. 26. Rozwiązanie musi zezwalać na połączenia przychodzące do udziałów administracyjnych po protokole SMB. 27. Rozwiązanie musi odmawiać połączenia starym (nieobsługiwanym) dialektom protokołu SMB oraz zabezpieczeniom tego protokołu bez rozszerzeń zabezpieczeń. 28. Rozwiązanie musi umożliwiać komunikację z usługą menadżera konta zabezpieczeń, urząd zabezpieczeń lokalnych, rejestr zdalny, service control manager, usługą serwera i innymi usługami. 29. Rozwiązanie musi umożliwiać zdefiniowanie listy aplikacji, dla których jest przeprowadzane filtrowanie protokołu SSL/TLS. 30. Rozwiązanie musi umożliwiać określenie białej listy domen dla których analiza

	protokoły SSL/TLS nie będzie wykonywana. 31. Rozwiązanie musi być wyposażona w mechanizm zarządzania podłączanymi do serwera nośnikami zewnętrznymi. 32. Rozwiązanie musi natywnie wspierać środowiska klastrowe. 33. Rozwiązanie musi wykorzystywać mechanizmy WMI w celu przekazywania informacji o swojej pracy do zewnętrznych systemów SIEM. 34. Rozwiązanie musi być wyposażona w mechanizmy auto ochrony swoich procesów przed ich ewentualnym wyłączeniem przez szkodliwe oprogramowanie. 35. Rozwiązanie musi zapewniać ochronę plików w czasie rzeczywistym, serwera na jakim jest zainstalowana. 36. Rozwiązanie musi umożliwiać skanowanie na żądanie zasobów serwera plików na jakim jest zainstalowana. 37. Rozwiązanie musi być wyposażone w mechanizm ochrony antyspamowej i antywirusowej pochodzący od jednego producenta. 38. Rozwiązanie musi być wyposażone w graficzny interfejs służący konfiguracji, dostępnych funkcjonalności. 39. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach oraz procesów. 40. Administrator ma możliwość dodania wykluczenia ze skanowania po tzw. HASH'u, wskazującym bezpośrednio na określoną infekcję, a nie konkretny plik. 41. Rozwiązanie musi umożliwiać zaawansowane skanowanie przy użyciu interfejsu AMSI. 42. Rozwiązanie musi posiadać wbudowany skaner UEFI. 43. Rozwiązanie musi posiadać wbudowany skaner skryptów JavaScript wykonywanych przez przeglądarki internetowe. 44. Rozwiązanie musi posiadać wbudowaną technologię monitorowania zdarzeń bezpieczeństwa związanych z zagrożeniami typu malware, exploit, PUA, podłączenia do sieci Botnet i in. za pomocą dedykowanej konsoli. 45. Rozwiązanie musi umożliwiać analizę zagrożeń przez porównanie skanowanych plików z białą i czarną listą obiektów w chmurze producenta. 46. Rozwiązanie musi umożliwiać określenie plików i folderów, które nigdy nie będą przesyłane do producenta w celu analizy, np. plików zawierających informacje poufne. 47. Rozwiązanie musi umożliwiać zapisywanie informacji diagnostycznych w dziennikach dla aparatu antyspamowego. 48. Rozwiązanie musi być wyposażone we wbudowany mechanizm greylistingu (szarej listy). 49. Rozwiązanie w celu ochrony antyspamowej musi wykorzystywać co najmniej bazy RBL,DNSBL, reputację poczty na podstawie oceny producenta. 50. Rozwiązanie musi umożliwiać tworzenie listy zaufanych domen, nadawców oraz adresów IP nadawców poczty. 51. Rozwiązanie musi umożliwiać tworzenie reguł blokujących konkretne zestawy znaków dialektycznych. 52. Rozwiązanie musi umożliwiać tworzenie czarnej listy domen, z którymi komunikacja będzie blokowana. 53. Rozwiązanie musi umożliwiać tworzenie ignorowanej listy adresów IP. 54. Rozwiązanie musi umożliwiać aktywację za pomocą dedykowanego pliku licencji offline. 55. Rozwiązanie musi umożliwiać aktywację za pomocą poświadczeń administratora licencji, konta utworzonego na dedykowanym portalu producenta. 56. Rozwiązanie musi weryfikować dostępność poprawek dla systemu operacyjnego Windows na jakim jest zainstalowana.

	57. Administrator musi posiadać możliwość konfiguracji jaki typ brakujących poprawek dla systemu operacyjnego ma być monitorowany. 58. Rozwiązanie musi być wyposażona w dedykowany moduł wiersza poleceń, umożliwiający wykonywanie zadań za pomocą skryptów. 59. Zwiększenie wydajności oraz przyśpieszenie skanowania maszyn wirtualnych oparte na technologii współdzielenia pamięci lokalnej. 60. Rozwiązanie musi umożliwiać eksport oraz import konfiguracji z poziomu GUI. 61. Rozwiązanie musi być wyposażone we wbudowane narzędzie diagnostyczne umożliwiające Administratorowi zebranie informacji na temat: a. uruchomionych procesów, b. ważnych wpisów w rejestrze, c. informacji na temat systemu operacyjnego, d. połączeń sieciowych, 62. Musi istnieć możliwość filtrowania wyświetlanych w narzędziu informacji w poziomach od 1-9. 63. Narzędzie musi umożliwiać wyświetlanie również ukrytych procesów na komputerze na którym generowany jest log. 64. Rozwiązanie musi tworzyć automatyczne wykluczenia dla krytycznych elementów serwera. 65. Administrator musi mieć możliwość przesłania podejrzanego pliku do producenta w celu poddania go analizie. 66. Do przesłania próbki nie może być wykorzystywany klient poczty email. 67. Rozwiązanie musi wykorzystywać do ochrony mechanizmy chmurowe, umożliwiające wykorzystanie reputacji plików analizowanych przez producenta. 68. Rozwiązanie musi automatycznie przesyłać powiadomienia o zdarzeniach pocztą e-mail na wskazany adres e-mailowy. 69. Musi istnieć możliwość zdefiniowania wykorzystywanego zestawu znaków. W tym co najmniej: Unicode (UTF-8), Ascii (7-bit), Japanese (ISO-2022-JP), lokalne. 70. Rozwiązanie musi rejestrować wszystkie dane transmitowane za pośrednictwem funkcji ochrony sieci w formacie PCAP. 71. Rozwiązanie musi umożliwiać zarejestrowanie dodatkowych informacji na temat systemu operacyjnego, na przykład dotyczące uruchomionych procesów, aktywności procesora o działania dysku. 72. Rozwiązanie musi rejestrować komunikację produktu z serwerami licencji producenta. 73. Rozwiązanie musi tworzyć log ochrony protokołu SMTP. 74. Rozwiązanie dla RMM (Remote Monitoring and Management). 75. Musi istnieć możliwość administracji zdalnej rozwiązaniem do ochrony IBM Domino za pomocą centralnej konsoli administracyjnej, pochodzącej od tego samego producenta. **Ochrona serwera pocztowego MS Exchange:** 1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych. 2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019. 3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub. 4. Rozwiązanie musi umożliwiać Administratorowi na etapie instalacji wybór komponentów jakie mają być zainstalowane. 5. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange. 6. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange

	przy pomocy VSAPI. 7. Rozwiązanie musi mieć możliwość zdefiniowania ilości wątków skanujących w celu optymalizacji pracy serwera. Liczba wątków skanowania musi wynosić od 1 do 21. 8. Rozwiązanie musi zapewnić skanowanie przed zapisaniem wiadomości w bazie danych przy pomocy transport agenta. 9. W przypadku wykrycia wirusa/blokowania wiadomości rozwiązanie musi umożliwić usunięcie wiadomości/ załącznika, podmianę załącznika na czysty plik zawierający jedynie informację o infekcji. 10. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum. 11. Rozwiązanie musi posiadać możliwość tworzenia białych i czarnych list domen/adresów IP, adresów e-mail. 12. Rozwiązanie musi posiadać możliwość akceptacji białych list stworzonych na poziomie serwera MS Exchange. 13. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty. 14. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty. 15. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja. 16. Program ma posiadać mechanizm greylisting (szara lista). 17. Rozwiązanie musi posiadać możliwość tworzenia wyjątków dla mechanizmu szarej listy. 18. Rozwiązanie musi posiadać możliwość stworzenia kwarantanny poczty per użytkownik. 19. Kwarantanna musi być dostępna dla użytkownika końcowego za pośrednictwem przeglądarki WWW. 20. Pliki zapisywane w katalogu kwarantanny muszą być szyfrowane. 21. Użytkownik końcowy musi posiadać możliwość zarządzania wiadomościami znajdującymi się w kwarantannie w tym co najmniej, mieć możliwość uwolnienia wiadomości z kwarantanny, jej usunięcia lub pozostawienia w kwarantannie. 22. Administrator musi mieć możliwość wglądu w globalną kwarantannę z poziomu interfejsu aplikacji oraz przeglądarki WWW. 23. Rozwiązanie musi umożliwiać przesyłanie raportów dotyczących plików poddanych kwarantannie na wskazany adres e-mail. 24. Rozwiązanie musi umożliwiać pominięcie reguł kwarantanny podczas zwolnienia wiadomości e-mail w środowisku klastrowym. 25. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików serwera „na żądanie” lub według harmonogramu. 26. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 27. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami. 28. Rozwiązanie musi posiadać wbudowaną technologię ochrony przed atakami typu backscatter. 29. Rozwiązanie musi umożliwiać zaawansowane skanowanie przy użyciu interfejsu AMSI. 30. Rozwiązanie musi posiadać wbudowany skaner UEFI.

	31. Rozwiązanie musi umożliwiać skonfigurowanie wyjątków ochrony przed atakami sieciowymi (IDS). 32. Rozwiązanie musi umożliwiać wykrywanie włamań wykorzystujących protokoły: SMB, RPC, RDP i informować użytkownika o wykryciu ataku. 33. Rozwiązanie musi wyświetlać powiadomienia po wykryciu ataku. 34. Rozwiązanie musi zezwalać na połączenia przychodzące do udziałów administracyjnych po protokole SMB. 35. Rozwiązanie musi odmawiać połączenia starym (nieobsługiwanym) dialektom protokołu SMB oraz zabezpieczeniom tego protokołu bez rozszerzeń zabezpieczeń. 36. Rozwiązanie musi umożliwiać komunikację z usługą menadżera konta zabezpieczeń, urząd zabezpieczeń lokalnych, rejestr zdalny, service control manager, usługą serwera i innymi usługami. 37. Rozwiązanie musi posiadać wbudowany skaner skryptów JavaScript, wykonywanych przez przeglądarki internetowe. 38. Rozwiązanie musi umożliwiać zdefiniowanie listy aplikacji, dla których jest przeprowadzane filtrowanie protokołu SSL/TLS. 39. Rozwiązanie musi umożliwiać określenie białej listy domen, dla których analiza protokoły SSL/TLS nie będzie wykonywana. 40. Rozwiązanie musi umożliwiać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 41. Rozwiązanie musi umożliwiać skanowanie plików spakowanych i skompresowanych 42. Rozwiązanie musi posiadać wbudowaną technologię monitorowania zdarzeń bezpieczeństwa związanych z zagrożeniami typu malware, exploit, PUA, podłączenia do sieci Botnet. 43. Musi być możliwe uruchamianie modułu ochrony przed złośliwym oprogramowaniem w ramach usługi chronionej systemu Windows (dla systemów Windows Server 2012 R2 lub nowszych). 44. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 45. Rozwiązanie musi wykorzystywać technologię chmury w celu przyśpieszenia reakcji na nowe zagrożenia oraz optymalizacji samego procesu skanowania. 46. Rozwiązanie musi umożliwiać analizę zagrożeń przez porównanie skanowanych plików z białą i czarną listą obiektów w chmurze producenta. 47. Rozwiązanie musi umożliwiać wybór jakie typy podejrzanych próbek będą przesyłane do producenta. W tym co najmniej: pliki wykonywalne, archiwa, skrypty, możliwy SPAM. 48. Rozwiązanie musi umożliwiać określenie plików i folderów, które nigdy nie będą przesyłane do producenta w celu analizy, np. plików zawierających informacje poufne. 49. Rozwiązanie musi umożliwiać zapisywanie informacji diagnostycznych w dziennikach dla aparatu antyspamowego. 50. Rozwiązanie musi być wyposażone w mechanizm chroniący serwer przed exploitami i atakami typu 0-day. 51. Rozwiązanie musi posiadać zaawansowany skaner pamięci umożliwiający wykrywanie zagrożeń próbujących działać na poziomie pamięci operacyjnej serwera. 52. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS). 53. Rozwiązanie musi w natywny sposób wspierać środowiska klastrowe. 54. Rozwiązanie musi umożliwiać wskazanie zewnętrznych lokalizacji w których przechowywane będą moduły i aktualizacje programu. 55. Rozwiązanie musi wspierać WMI za pomocą których może przekazywać podstawowe informacje na temat swojej pracy do zewnętrznych systemów np. SIEM.

	56. Rozwiązanie musi skanować i oczyszczać w czasie rzeczywistym pocztę przychodzącą i wychodzącą, która jest obsługiwana przy pomocy programu Microsoft Outlook zainstalowanego lokalnie na serwerze pocztowym. 57. Rozwiązanie musi posiadać wbudowaną ochronę przed atakami typu phishing w wiadomościach e-mail. 58. Rozwiązanie musi umożliwiać skanowanie w środowiskach hybrydowych opartych na MS Office 365. 59. Rozwiązanie musi umożliwiać ochronę dostępu do urządzeń według zdefiniowanych reguł w określonych przedziałach czasu. 60. Rozwiązanie musi tworzyć log ochrony protokołu SMTP. 61. Rozwiązanie musi mieć możliwość utworzenia kilku zadań skanowania (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (metody skanowania, obiekty skanowania, czynności). 62. Rozwiązanie musi umożliwiać aktualizację modułów ochrony bez konieczności reinstalacji całego programu. 63. Rozwiązanie musi uruchamiać jeden skaner uruchamiany w pamięci, do którego odnoszą się wszystkie monitory skanujące i skanery na żądanie. 64. Rozwiązanie musi mieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach oraz procesów. 65. Administrator ma możliwość dodania wykluczenia ze skanowania po tzw. HASH'u, wskazującym bezpośrednio na określoną infekcję, a nie konkretny plik. 66. Rozwiązanie musi być wyposażone w dwa niezależnie pracujące mechanizmy analizy heurystycznej (standardowa i zaawansowana heurystyka). 67. Administrator musi posiadać możliwość używania jednego poziomu analizy heurystycznej lub obu poziomów jednocześnie. 68. Rozwiązanie musi umożliwiać automatyczne wysyłanie nowych zagrożeń (wykrytych przez heurystykę) do laboratorium producenta przez program antywirusowy – nie wymaga ingerencji użytkownika. 69. Wysyłanie nowych zagrożeń musi być możliwe za pomocą interfejsu rozwiązania i nie może do tego celu wykorzystywać klienta pocztowego zainstalowanego w systemie. 70. Rozwiązanie musi umożliwiać wysyłanie wraz z próbką adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 71. W przypadku wykrycia wirusa, ostrzeżenie może zostać wysłane do administratora poprzez e- mail. 72. Rozwiązanie musi posiadać wbudowany dziennik zdarzeń rejestrujący informacje na temat znalezionych wirusów, dokonanych aktualizacji baz wirusów i wersji oprogramowania. 73. Administrator musi mieć możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu. 74. Możliwość zabezpieczenia hasłem musi obejmować wyłączenie rozwiązania antywirusowego oraz jego odinstalowanie. 75. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 76. Rozwiązanie musi być dostępne z Internetu, lokalnego zasobu sieciowego, nośnika CD/DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP). 77. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. 78. Rozwiązanie musi wspierać aktualizacje za pośrednictwem serwera Proxy.

	79. Administrator musi posiadać możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami. 80. Rozwiązanie musi rejestrować wszystkie dane transmitowane za pośrednictwem funkcji ochrony sieci w formacie PCAP. 81. Rozwiązanie musi umożliwiać zarejestrowanie dodatkowych informacji na temat systemu operacyjnego, na przykład dotyczące uruchomionych procesów, aktywności procesora o działania dysku. 82. Rozwiązanie musi rejestrować komunikację produktu z serwerami licencji producenta. 83. Rozwiązanie musi automatycznie przesyłać powiadomienia o zdarzeniach pocztą e-mail na wskazany adres e-mailowy. 84. Musi istnieć możliwość zdefiniowania wykorzystywanego zestawu znaków. W tym co najmniej: Unicode (UTF-8), Ascii (7-bit), Japanese (ISO-2022-JP), lokalne. 85. Rozwiązanie musi posiadać wsparcie dla RMM (Remote Monitoring and Management). 86. Rozwiązanie musi posiadać możliwość zdalnej administracji za pomocą konsoli administracji zdalnej. 87. Rozwiązanie musi posiadać wbudowany, dedykowany moduł command line umożliwiający konfigurację oraz uruchamianie zadań zainstalowanej aplikacji. 88. Rozwiązanie musi być wyposażone w narzędzie umożliwiające wygenerowanie raportu dotyczącego stanu komputera, w tym co najmniej zainstalowanych aplikacji, uruchomionych procesów, ważnych wpisów w rejestrze i uruchomionych usług. 89. Do administracji zdalnej musi być wykorzystywany dedykowany agent. 90. Agent musi komunikować się z serwerem administracji zdalnej w bezpieczny sposób uniemożliwiający podsłuch komunikacji. 91. Skuteczność programu ma być potwierdzona nagrodami niezależnych organizacji (np. VB100, ISCA labs, Check Mark). 92. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. **Administracja zdalna w chmurze:** 1. Serwer administracyjny musi być dostępny w chmurze producenta oprogramowania antywirusowego. 2. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia przechowywanych danych. 3. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW. 4. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL. 5. Serwer Administracyjny musi obsługiwać przynajmniej 50 000 stacji roboczych/serwerów. 6. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 7. Serwer administracyjny musi posiadać wsparcie dla „VDI” oraz „Golden Master Image”. 8. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 9. Administrator musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 10. Administrator musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap. 11. Serwer administracyjny musi pozwalać na zarządzanie programami

	zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android. 12. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci. 13. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. 14. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające. 15. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania. 16. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. 17. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play. 18. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS. 19. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego. 20. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 21. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 22. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. 23. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie generowania raportów i usuwania stacji roboczych. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej. 24. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji. 25. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych. 26. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT. 27. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia

	komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej. 28. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej. 29. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 30. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 31. Szablon grupy dynamicznej musi umożliwiać zdefiniowane przedziału czasowego kiedy grupa dynamiczna ma działać. 32. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania. 33. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. 34. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta. 35. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej. 36. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji. 37. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce. 38. Serwer administracyjny musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 39. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów. 40. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie. 41. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy. 42. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania. 43. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów. 44. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny. 45. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF i CSV. 46. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. 47. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów. 48. Powiadomienia mailowe mają być wysyłane w formacie HTML.

	49. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń. 50. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email. 51. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu. 52. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji. 53. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych. 54. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu. 55. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela. 56. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami. 57. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli. 58. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych. 59. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta. 60. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli. 61. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania. 62. Serwer musi wspierać wysyłanie logów do systemu SYSLOG. 63. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych. 64. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk. 65. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal). 66. Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów. **Ochrona poprzez dwuskładnikowe uwierzytelnianie:** 1. Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: 2008 /2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials/ Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 /Windows Server 2019 Essentials / Windows Server 2022. 2. Rozwiązanie musi wspierać system operacyjne Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11.

	3. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows. 4. Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019. 5. Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016. 6. Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 /2019. 7. Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access. 8. Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Access. 9. Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access. 10. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS. 11. Oprogramowanie musi integrować się z systemem Windows Server poprzez konsolę MMC (Microsoft Managment Console). 12. Moduł zarządzania uwierzytelnianiem się użytkowników musi integrować się z wbudowanym w systemie Windows Server modułem do zarządzania kontami użytkowników (ADUC) w postaci dodatkowej zakładki we właściwościach użytkownika. 13. Administrator musi mieć możliwość określenia z jakiej metody uwierzytelniania użytkownicy będą korzystać: – dwuskładnikowe uwierzytelnianie poprzez użycie aplikacji mobilnej zainstalowanej na urządzeniu mobilnym użytkownika, – dwuskładnikowe uwierzytelnianie poprzez wiadomości SMS wysyłane do użytkowników, – klasyczna uwierzytelnianie (przy użyciu nazwy użytkownika i hasła). 14. Administrator musi mieć możliwość wysłania w postaci wiadomości SMS odnośnika, za pomocą którego użytkownik może pobrać i zainstalować dedykowaną aplikację mobilną wspierającą systemy mobilne opisane w sekcji Aplikacja mobilna pkt. 1 15. Dwuskładnikowe uwierzytelnianie nie może wymagać od użytkownika instalacji aplikacji mobilnej w telefonie – wówczas jednorazowe hasła muszą być przesyłane do użytkownika w postaci wiadomości SMS. 16. Dodatek w module ADUC musi wyświetlać informację co najmniej o dniu i godzinie ostatniej próby logowania oraz ostatniej nieudanej próby logowania użytkownika. 17. Oprogramowanie musi posiadać mechanizm zabezpieczający przed atakiem typu brute-force, które po określonej liczbie prób nieudanego logowania musi automatycznie zablokować możliwość uwierzytelnienia się dla danego użytkownika. 18. Administrator musi mieć możliwość odblokowania konta użytkownika w celu umożliwienia ponownego dostępu. 19. Administrator musi mieć możliwość wymuszenia zabezpieczenia aplikacji mobilnej za pomocą kodu PIN lub za pomocą danych biometrycznych – wówczas każdy użytkownik instalujący aplikację mobilną bez nadania kodu PIN nie będzie mógł generować jednorazowych haseł (OTP). 20. Administrator musi mieć możliwość podglądu informacji na temat: – aktualnego stanu licencji, – ilości wykorzystanych licencji (użytkowników), – ilości pozostałych do wykorzystania wiadomości SMS. 21. Oprogramowanie przy użyciu serwera RADUIS musi umożliwiać dostęp do zabezpieczonych zasobów za pomocą klasycznej metody uwierzytelnienia (nazwa użytkownika i hasła).

	22. Administrator musi mieć możliwość wyboru, którzy użytkownicy będą korzystać z dwuskładnikowego uwierzytelniania. 23. Administrator musi mieć możliwość ograniczenia dostępu przy uwierzytelnianiu metodą RADIUS do grupy użytkowników wskazanych w konfiguracji. 24. Jednorazowe hasło (OTP) generowane przez użytkowników powinno być unikalne i może być użyte tylko raz – nie dopuszcza się wielokrotnego użycia tego samego OTP. 25. Do wysyłania wiadomości SMS nie może być wymagane posiadanie własnej bramy SMS i centrali GSM. 26. Wysyłanie wiadomości SMS z hasłami jednorazowymi musi odbywać się z infrastruktury producenta rozwiązania. 27. Wysyłanie wiadomości musi być możliwe w przypadku telefonów pracujących w roamingu. 28. Producent musi udostępnić API pozwalające programistom na zintegrowanie rozwiązania z serwisem web lub oprogramowaniem wykorzystującym uwierzytelnianie w oparciu o usługę Active Directory. 29. Producent musi udostępniać SDK w celu umożliwienia programistom implementacji dwuskładnikowego uwierzytelniania dla środowisk nie wykorzystujących usługi Active Directory do uwierzytelniania użytkowników (np. wykorzystujących własną bazę danych z użytkownikami). 30. SDK musi być dostarczone zarówno dla platformy Microsoft .NET jak i języków programowania PHP i Java. **Aplikacja mobilna:** 1. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej). 2. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN. 3. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline. 4. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego użytkowników poprzez dwuskładnikowe uwierzytelnianie. 5. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. **Ochrona serwera – Linux:** <u>Architektura rozwiązania</u> 1. Rozwiązanie musi posiadać skaner antywirusowy i antyspyware. 2. Rozwiązanie musi umożliwiać skanowanie plików, plików spakowanych i archiwów samorozpakowujących. 3. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu. 4. Rozwiązanie musi posiadać wbudowany mechanizm typu „watchdog”. Monitoruje on tzw. stan zdrowia poszczególnych mikro-serwisów i automatycznie przeładowuje je w przypadku wykrycia zakłóceń w pracy mikro-serwisu. 5. Architektura rozwiązania musi pozwalać na uruchamianie poszczególnych mikroserwisów, tylko na czas realizacji funkcjonalności przez nie realizowanych, co pozwala w znaczącym stopniu ograniczyć wykorzystanie zasobów systemu operacyjnego.

	6. Rozwiązanie musi wspierać wieloprocesorową i wielordzeniową architekturę, w celu zapewnienia maksymalnego zwiększenia wydajności. 7. Rozwiązanie musi posiadać wsparcie dla SecureBoot-a. 8. Rozwiązanie musi być wyposażone w moduł ochrony systemu plików w czasie rzeczywistym. Moduł nie może wymagać instalowania jakichkolwiek dodatkowych komponentów w systemie operacyjnym. Wszystkie komponenty muszą być instalowane w systemie, podczas instalacji z dostarczonego instalatora binarnego. 9. Silnik ochrony systemu plików w czasie rzeczywistym musi stanowić dodatkowy moduł jądra systemu Linux i musi być dodawany do jądra, podczas procesu instalacji oprogramowania antywirusowego. 10. Ochrona systemu plików w czasie rzeczywistym musi być zapewniona nieprzerwanie od uruchomienia produktu i obejmuje skanowanie zarówno dysków lokalnych jak i zmapowanych dysków sieciowych. 11. Silnik skanujący musi działać wyłącznie z wykorzystaniem 64-bitowej architektury. 12. Rozwiązanie musi być w pełni zgodne z modułem SELinux, pracującym zarówno w trybie „Permissive" jak i „Enforcing". 13. Rozwiązanie podczas procesu instalacji, musi dodawać i konfigurować własne polityki modułu SELinux, które są kompatybilne z następującymi dystrybucjami systemów Linux: Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 8, Centos 7. 14. Wszystkie mechanizmy bezpieczeństwa rozwiązania muszą wspierać system informowania o zagrożeniach w czasie rzeczywistym. System ten pozwala na weryfikowanie reputacji plików oraz procesów i identyfikację nowych i nieznanych zagrożeń. 15. Skaner systemu plików w czasie rzeczywistym musi działać dla operacji obsługi plików, dla co najmniej takich operacji jak: dostęp do pliku, utworzenie (zapisanie) pliku. 16. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 17. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku. 18. Rozwiązanie musi być wyposażone we własny wiersz polecenia (CLI). Polecenia muszą być odpowiedzialne co najmniej za: skanowanie na żądanie, konfigurację mechanizmów bezpieczeństwa, uruchamianie aktualizacji, przeglądanie logów aplikacji, konfigurację graficznego interfejsu użytkownika, obsługę kwarantanny plików. 19. Rozwiązanie musi wspierać system plików zamontowany z flagą „noexec". 20. Rozwiązanie musi pozwalać na uruchamianie zadań skanowania działających „w tle", z możliwością ustawienia dla nich niskiego priorytetu. 21. Zadania skanowania nie mogą zmieniać znacznika dostępu do plików. <u>Interfejs graficzny</u> 1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 2. Lokalna konsola administracyjna musi działać w oparciu o dynamicznie generowaną zawartość tworzoną z wykorzystaniem następujących technologii: React/Node.js, HTML5. 3. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 4. Lokalna konsola administracyjna musi zapewniać bezpieczne połączenie działające w oparciu o protokół HTTPS. 5. Lokalna konsola administracyjna musi umożliwiać uruchomienie jej, na wskazanym porcie TCP. 6. Logowanie do lokalnej konsoli administracyjnej musi być realizowane, poprzez

	podanie danych w postaci nazwy użytkownika i zdefiniowanego dla niego hasła. 7. Lokalna konsola administracyjna musi zapewniać funkcjonalność zweryfikowania stanu licencji i informacji na jej temat. 8. Z poziomu lokalnej konsoli administracyjnej musi być możliwość zarządzania, wbudowanym modułem menadżera kwarantanny. 9. Lokalna konsola administracyjna musi zapewniać możliwość przełączenia wersji językowej konsoli, na etapie logowania. Lokalna konsola administracyjna musi posiadać interfejs, co najmniej języku: polskim, angielskim, niemieckim, francuskim, hiszpańskim, japońskim. Skanowanie sieciowych systemów plików 1. Rozwiązanie musi pozwalać na skanowanie plików składowanych i obsługiwanych przez zewnętrzne rozwiązania obsługi danych typu NAS / SAN. 2. Rozwiązanie nie może wymagać instalacji jakichkolwiek dodatkowych modułów na rozwiązaniach typu NAS / SAN, a skanowanie plików musi się odbywać wyłącznie w oparciu o protokół ICAP. 3. Rozwiązanie musi umożliwiać zmianę domyślnego portu protokołu ICAP. 4. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. Instalacja 1. Rozwiązanie musi wspierać mechanizm instalacji zdalnej, realizowanej przez narzędzia do orkiestracji systemami operacyjnymi. Wspieranymi narzędziami muszą być co najmniej: Puppet, Chef, Ansible. 2. Rozwiązanie musi być wyposażone w mechanizm automatycznej aktualizacji komponentów programu. 3. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 4. Rozwiązanie musi wspierać następujące systemy operacyjne: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux oraz Alma Linux. Licencjonowanie 1. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 2. Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji rozwiązania w trybie offline. **Ochrona serwera Windows:** 1. Rozwiązanie musi posiadać wsparcie dla systemów Microsoft Windows Server 2012 i nowszych. 2. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. 3. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 4. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami. 6. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje. 7. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.

	8. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu. 9. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). 10. Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 11. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 12. Rozwiązanie ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 13. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych. 14. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych. 15. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 16. Rozwiązanie musi wspierać mechanizm klastrowania. 17. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS). 18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, d. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. 19. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. 20. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. 21. Rozwiązanie musi posiadać zaawansowany skaner pamięci. 22. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych. 23. Rozwiązanie musi oferować możliwość skanowania dysków sieciowych typu NAS. 24. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze. 25. Rozwiązanie musi umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

	26. Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 27. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia. 28. Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia. 29. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. 30. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego. 31. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. 32. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 33. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. 34. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. 35. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych. 36. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. 37. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji. 38. Rozwiązanie ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). 39. Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 40. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 41. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie. 42. Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. 43. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 44. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 45. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.

	46. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. 47. Rozwiązanie musi posiadać możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło. 48. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo. 49. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji. 50. Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. 51. Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń. 52. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. 53. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. 54. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 55. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 56. Rozwiązanie musi oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. 57. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 58. Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera. 59. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji. 60. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. 61. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. 62. Rozwiązanie musi być wyposażone w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). 63. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 64. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.

	65. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 66. Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania. 67. Rozwiązanie musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść". 68. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 69. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia. 70. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 71. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 72. Rozwiązanie musi posiadać ochronę przed przyłączeniem komputera do sieci botnet. 73. Rozwiązanie musi mieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 74. Rozwiązanie musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów. 75. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. 76. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów. 77. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 78. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. **Zarządzanie podatnościami i aktualizacjami:** 1. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach. 2. Baza wykrywanych podatności musi zawierać minimum 35000 CVE. 3. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych komponentów na stacjach końcowych. 4. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie. 5. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum: a. nazwę aplikacji lub systemu operacyjnego, b. punktacje CVSS, c. opis wykrytej podatności, d. wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta. 6. Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach. 7. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji. 8. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane

	tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania. 9. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji niepodlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich – ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania. 10. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach. 11. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze. 12. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania. 13. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania. 14. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności. **Ochrona usługi Microsoft 365:** 1. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams. 2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Micosoft 365. 3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną. 4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci. 5. Rozwiązanie musi być dostępny w języku polskim. 6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej: a. użytkowników, otrzymujących najwięcej spamu, b. użytkowników, otrzymujących najwięcej wiadomości typu „phishing”, c. użytkowników, otrzymujących największą ilość szkodliwego oprogramowania, d. kont użytkowników, które mogę być podejrzane. 7. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive. 8. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej: a. jaka ilość wiadomości została przeskanowania, b. wynik skanowania poszczególnej wiadomości, c. czynność podjęta przez rozwiązanie. 9. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o: a. zagrożeniach, które zostały wykryte, b. na jakim koncie zostały wykryte, c. jakie zagrożenie zostało wykryte, d. podjętą czynność. 10. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive. 11. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem. 12. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych

	do rozwiązania tenantów lub do poszczególnych grup i użytkowników. 13. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej: a. wykorzystania do analizy mechanizmów chmurowych, tego samego producenta, b. wprowadzenia białych i czarnych list adresów ochrony Exchange'a Online, c. dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing. 14. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day. 15. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta. 16. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. 17. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta. 18. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka. **Wdrożenie dostarczonego oprogramowania równoważnego:** Zamawiający wymaga aby dostarczone oprogramowanie zostało zainstalowane i skonfigurowane wraz z wdrożeniem polityk ochrony w środowisku Zamawiającego przez zespół Wykonawcy stacjonarnie w siedzibie Zamawiającego. Obejmuje to: zaprojektowanie w współpracy z Zamawiającym polityk ochrony, z uwzględnieniem środowiska Zamawiającego, dezinstalację posiadanego obecnie oprogramowania antywirusowego, instalację nowego oprogramowania w środowisku Zamawiającego, implementację polityk na stacjach roboczych i serwerach. Testy poprawności działania i kompatybilności ze środowiskiem Zamawiającego. Przygotowanie i przekazanie Zamawiającemu dokumentacji powykonawczej. Warsztaty z obsługi oprogramowania. Zamawiający wymaga aby warsztaty z zakresu instalacji, konfiguracji i obsługi oprogramowania zrealizowane były przez ośrodek posiadający autoryzację producenta oprogramowania i przeprowadzone były dla 2 administratorów Zamawiającego, trwały co najmniej 28 h (7 dni x 4 h) w tym wykłady i warsztaty praktyczne, zawierały omówienie funkcji oprogramowania, metod wdrożenia, konfiguracji i czynności administracyjnych, wydany był certyfikat lub zaświadczenie wystawione przez ośrodek szkoleniowy, świadczące o ukończeniu szkolenia. Zamawiający wymaga aby warsztaty przeprowadzone były w trybie stacjonarnym w siedzibie Zamawiającego na sprzęcie Wykonawcy. Warsztaty muszą się odbyć w maksymalnym terminie 2 tygodni liczonym od dnia podpisania protokołu odbioru wdrożenia systemu backupu. Wsparcie techniczne. Wykonawca zobowiązuje się do świadczenia usług wsparcia technicznego w okresie 24 miesięcy licząc od dnia podpisania protokołu odbioru na następujących warunkach: czas reakcji w przypadku krytycznego błędu (awarii) oprogramowania, gdy system o znaczeniu krytycznym dla Zamawiającego jest niedostępny lub nie działa – będzie nie dłuższy niż 2 godziny od momentu zgłoszenia, czas reakcji w przypadku bardzo poważnego błędu (awarii) oprogramowania, gdy system o znaczeniu produkcyjnym dla Zamawiającego jest dostępny w ograniczonym zakresie – będzie nie dłuższy niż 8 godzin od momentu zgłoszenia. W okresie trwania wsparcia technicznego Wykonawca zapewni Zamawiającemu dostęp do nowych wersji oprogramowania. Przyjmowanie zgłoszeń serwisowych i liczenie czasu reakcji realizowane będzie w godzinach od 7:00 do 16:00 w dni robocze, od poniedziałku do piątku.

CZĘŚĆ VI – SYSTEM NAC

1. System NAC Network Access Control do zarządzania dostępem użytkowników i urządzeń do sieci – 1 szt.

Minimalne parametry	
Urządzenie do ochrony sieci komputerowej typu NAC	
Parametry funkcjonalne i techniczne. Gwarancja i serwis.	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.). 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. 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. <u>Wymagania ogólne rozwiązania NAC</u> 1. Ma zapewnić widoczność i monitorowanie wszystkich urządzeń pracujących w sieci lokalnej oraz powiadamiać o nowych urządzeniach pojawiających się w sieci. 2. Musi zapewniać automatyczne blokowanie komunikacji sieciowej między nowym, niezaufanym urządzeniem a zaufanymi, zarządzanymi urządzeniami pracującymi w sieci. 3. 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. 4. Musi umożliwiać odbieranie komunikatów bezpieczeństwa z innych systemów bezpieczeństwa (np. firewalla) i automatyczne blokowanie na tej podstawie wskazanych urządzeń w sieci. 5. 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. 6. Stosowany mechanizm blokowania musi wykorzystywać protokół ARP i działać całkowicie niezależnie od innych elementów infrastruktury sieciowej. 7. Rozwiązanie musi działać bezagentowo, bez konieczności instalowania jakichkolwiek agentów na urządzeniach w sieci oraz bez konieczności dokonywania zmian w infrastrukturze sieciowej.

	8. Rozwiązanie musi umożliwiać wysyłanie alertów do administratora za pomocą e-maila oraz SMS. 9. Rozwiązanie musi być zarządzane przez interfejs webowy, obsługiwany przeglądarką internetową. 10. Wymaga się, aby rozwiązanie było dostarczone w postaci sprzętowej (hardware appliance), wyposażonej w min. 4 porty 1GbE. System musi pozwalać na monitorowanie łącznie co najmniej 300 urządzeń. 11. Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej z odnawialnym wsparciem i konserwacją (support & maintenance). Wymaga się dostarczenia urządzenia sprzętowego, 300 licencji wieczystych oraz wsparcia technicznego i konserwacji na okres 1 roku. 12. Wsparcie techniczne i konserwacja musi obejmować naprawę/wymianę urządzenia w wypadku jego awarii, dostarczanie aktualizacji oprogramowania/firmware oraz pomoc techniczną producenta w dni robocze w godzinach pracy. 13. Kompletne rozwiązanie, czyli sprzęt, licencje oprogramowania i wsparcie techniczne muszą pochodzić od jednego producenta. <u>Wymagania szczegółowe – monitorowanie podsieci</u> 1. Rozwiązanie musi w czasie rzeczywistym raportować widoczność wszystkich urządzeń pracujących w monitorowanych podsieciach. 2. Rozwiązanie musi wykrywać nowe nieznane urządzenie, dołączające się do sieci LAN lub WLAN, w czasie nie dłuższym, niż 5 sekund oraz wysyłać powiadomienie mailowe do administratora. 3. Rozwiązanie musi wykrywać przypadki skanowania urządzeń i portów w monitorowanych podsieciach i blokować urządzenie inicjujące takie skanowanie. 4. Rozwiązanie musi posiadać funkcję pułapki sieciowej (honeypot), symulującą w każdej monitorowanej podsieci standardowe usługi sieciowe, co najmniej: ssh, telnet, ftp i smb. Rozwiązanie musi rejestrować każdą próbę zalogowania się do takiej symulowanej usługi, zapisując użytą nazwę użytkownika, hasło użytkownika i źródłowy MAC/IP. 5. 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. 6. 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. 7. Rozwiązanie musi obsługiwać VLANy, tj. umożliwiać monitorowanie przez jeden fizyczny interfejs sieciowy wielu podsieci, zdefiniowanych jako VLANy. <u>Wymagania szczegółowe – polityka bezpieczeństwa</u> 1. Rozwiązanie musi umożliwiać definiowanie polityki bezpieczeństwa, czyli określenie przez administratora, jakie warunki musi spełniać aktualny stan urządzenia, aby uzyskało ono określony dostęp do sieci. 2. 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. 3. Polityka bezpieczeństwa musi umożliwiać przypisanie do urządzenia jednego z trzech trybów dostępu do sieci: a. pełny dostęp, b. blokowanie (całkowity brak dostępu), c. ograniczony dostęp. 4. 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. 5. Rozwiązanie powinno automatycznie sprawdzać, które warunki polityki bezpieczeństwa spełnia urządzenie i na tej podstawie przypisywać do urządzenia właściwy zakres dostępu. 6. Zakres dostępu, wynikający ze spełnienia przez urządzenie danych warunków polityki bezpieczeństwa powinien być egzekwowany przez mechanizm kwarantanny. 7. Musi być możliwość łatwego, manualnego tworzenie białej listy adresów MAC, czyli listy urządzeń mogących bez żadnych ograniczeń ze strony NAC pracować w sieci. <u>Wymagania szczegółowe – mechanizm kwarantanny</u> 1. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenie, aby wyegzekwować ograniczenia dostępu do sieci, wynikające z polityki bezpieczeństwa. 2. Mechanizm kwarantanny powinien umożliwiać: a. całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, b. częściowe blokowanie komunikacji urządzenia z otoczeniem sieciowym, w zakresie definiowanym przez administratora przez wskazanie adresów IP i portów, z którymi urządzenie może się komunikować. 3. Mechanizm kwarantanny powinien blokować komunikację urządzenia w czasie nie dłuższym, niż 5 sekund od zaistnienia warunku, powodującego nałożenie kwarantanny. 4. 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. 5. Kwarantanna powinna być zdejmowana z urządzenia automatycznie, gdy spełni ono kryteria polityki bezpieczeństwa, pozwalające na pełny dostęp. 6. 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. 7. Awaria rozwiązania nie może powodować blokady komunikacji w sieci, tj w przypadku awarii rozwiązania wszystkie urządzenia mają mieć pełny dostęp do sieci. 8. Rozwiązanie musi umożliwiać włączenie i wyłączenie mechanizmu kwarantanny (blokowania komunikacji) w każdej monitorowanej podsieci osobno. <u>Wymagania szczegółowe – integracja z systemami zewnętrznymi</u> 1. Rozwiązanie musi umieć sprawdzić, czy urządzenia z systemem Windows są dołączone do domeny AD. 2. 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. 3. Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym poprawkami Windows i sprawdzanie statusu zainstalowanych poprawek na zarządzanych urządzeniach z systemem Windows. Wymagana jest możliwość

	integracji co najmniej z systemami: Microsoft WSUS. 4. 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, CrowdStrike, Cybereason, Eset, McAfee, SentinelOne, Sophos, Symantec, TrendMicro, Webroot. 5. Rozwiązanie musi umożliwiać wykorzystanie pozyskanych informacji, wymienionych w poprzedzających punktach 1-4, do definiowania polityki bezpieczeństwa. 6. Rozwiązanie musi umieć odbierać alerty przysyłane za pomocą e-mail lub syslog z innych urządzeń bezpieczeństwa (np. firewalla) i na podstawie zawartych w nich informacji blokować wskazane podejrzane urządzenie. <u>Wymagania szczegółowe – rejestracja urządzeń zewnętrznych: pracowników, gości i konsultantów (Captive Portal)</u> 1. 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. 2. Captive Portal musi umożliwiać pracownikom rejestrowanie urządzeń prywatnych (BYOD) i wnioskowanie o dostęp do sieci w ograniczonym zakresie, zdefiniowanym przez administratora. 3. Przy rejestracji przez pracowników ich prywatnych urządzeń, Captive Portal powinien umożliwiać użycie ich kont Active Directory. 4. Powinna istnieć możliwość ograniczenia ilości i rodzaju rejestrowanych przez pracownika prywatnych urządzeń. 5. Powinna być możliwość przypisania ograniczonego dostępu dla zarejestrowanych urządzeń prywatnych. 6. Captive Portal musi umożliwiać osobom nie będącym pracownikami (gościom lub konsultantom) wnioskowanie o ograniczony dostęp do sieci. 7. W przypadku rejestracji urządzeń gości powinna być możliwość rejestracji samodzielnie przez gościa oraz przez uprawnionego pracownika firmy. 8. Zarejestrowane urządzenia gości powinny automatycznie tracić przydzielony dostęp po upływie zdefiniowanego czasu. 9. Powinna istnieć możliwość ograniczenia ilości urządzeń rejestrowanych przez gościa. 10. Dla zarejestrowanych urządzeń gości powinna być możliwość ograniczenia, w jakich przedziałach czasu i z jakich podsieci będą one miały dostęp do sieci. 11. Dla urządzeń gości powinna być możliwość przypisania dostępu ograniczonego tylko do dostępu do internetu. 12. Dla urządzeń konsultantów powinna być możliwość przypisania dostępu ograniczonego do wybranych zasobów lokalnych. 13. 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. 14. Rozwiązanie musi przechowywać historyczne raporty dostępu do sieci użytkowników typu gość i konsultant. 15. 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 1. Rozwiązanie powinno oferować uwierzytelnianie administratora za pomocą dodatkowego składnika, oprócz hasła (2FA). 2. 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. 3. Rozwiązanie nie powinno pogarszać wydajności pracy przełączników i routerów, nie może wymagać współpracy z przełącznikami przez port mirroring czy port spanning. 4. Rozwiązanie nie powinno pogarszać wydajność łącz WAN. 5. Rozwiązanie nie powinno pogarszać wydajności pracy monitorowanych urządzeń w sieci. Wdrożenie Wymaga się, aby dostawca wdrożył rozwiązania w infrastrukturze Zamawiającego, w wymienionym poniżej zakresie, przeprowadzoną przez wykwalifikowanego inżyniera, certyfikowanego przez producenta rozwiązania: – instalacja i konfiguracja sprzętowego appliance'a, – szkolenie dla administratora rozwiązania, – wsparcie w języku polskim w trybie 8 godzin x 5 dni roboczych w okresie aktywnej subskrypcji wsparcia technicznego.

CZĘŚĆ VII – ZARZĄDZANIE LOGAMI

1. Oprogramowanie do gromadzenia i zarządzania logami – 1 szt.

Minimalne parametry	
Parametry funkcjonalne	1. Zamawiający wymaga, aby rozwiązanie do zbierania i analizowania logów zostało dostarczone w formie rozwiązania sprzętowego i posiadało dostęp przez interfejs web umożliwiający administratorom i operatorom wykorzystanie wszystkich jego funkcji. 2. Zamawiający wymaga aby rozwiązanie obsługiwało natywnie co najmniej urządzenia/oprogramowanie: Apache, Eset, Dell iDrac, FreeRADIUS, HPE iLo, BIND, Linux, Mikrotik, Microsoft Exchange, Microsoft SharePoint, Microsoft SQL, Microsoft Windows, MySQL, Nginx, OpenSSH server, Oracle DB, PostgreSQL, Sophos, SpamAssasin, Squid, Synology, VMware. 3. Zdarzenia z systemów Windows muszą być zbierane przez dedykowane oprogramowanie (tzw. agent) instalowane bezpośrednio na stacjach końcowych i wysyłające dane do centralnej instancji systemu. a) Agent Windows musi umożliwiać zbieranie logów zarówno z systemowego dziennika zdarzeń jak i z plików tekstowych w systemie Windows, b) Agent musi zapewniać zbieranie wszystkich danych związanych ze zdarzeniem w oryginalnej, niezmodyfikowanej formie (tzn. całość a nie tylko części zdarzenia). 4. Oferowane rozwiązanie musi umożliwiać filtrowanie zdarzeń (przykładowo odrzucanie nieistotnych) zbieranych przez agenta Windows jeszcze przed wysłaniem do centralnej instancji. Filtrowanie zdarzeń zbieranych przez agenta Windows musi być możliwe do skonfigurowania za pomocą programowania wizualnego. 5. Ilość agentów dla systemu Windows nie może być limitowana licencyjnie. Oferowane rozwiązanie musi być pozbawione limitowania pod kątem ilości

	zbieranych danych. 6. Wymagania wobec Agenta Windows: a) dostarczenie dokumentacji opisującej proces instalacji i konfiguracji agenta, b) po zainstalowaniu, nie może wymagać interwencji administratora na systemie końcowym – musi być centralnie zarządzany, a jego konfiguracja możliwa do przeprowadzenia z poziomu interfejsu graficznego web, bez konieczności ręcznego edytowania plików systemowych. Aktualizacja konfiguracji agenta musi być automatycznie dystrybuowana bezpośrednio z centralnej konsoli systemu, c) musi automatycznie tłumaczyć kody zdarzeń Windows na postać tekstową wynikającą ze zdefiniowanych słowników (przykładowo: Logon Type 2 = Interactive, Logon Type 3 = Network, etc.), d) musi posiadać bufor lokalny na wypadek utraty połączenia stacji końcowej z centralną instancją systemu. Dane, których nie udało się przekazać do centralnej instancji systemu, muszą zostać przekazane natychmiast po powrocie połączenia, również gdy stacja robocza była w między czasie restartowana, e) komunikacja pomiędzy agentem Windows, a centralną instancją systemu musi być zaszyfrowana (min. TLS 1.2), f) musi wspierać kolekcjonowanie nie tylko podstawowych zdarzeń z dziennika zdarzeń (Application, Security, Setup, System), ale także umożliwiać zbieranie logów z folderu Applications and Services Logs. Dodatkowo agent Windows musi umożliwiać pobieranie danych logów z plików tekstowych z systemu Windows, konfigurowane z centralnej instancji systemu, w tym możliwość wybrania ich formatu danych (przykładowo: dziennik zdarzeń, plik txt, dhcp, iis), g) musi automatycznie dodawać opis tekstowy do wszystkich zbieranych zdarzeń, dokładnie tak jak jest to prezentowane w Dzienniku Zdarzeń systemu Windows, h) musi umożliwiać zbieranie logów z płaskich plików w systemie, z którego zbierane są logi poprzez podanie ich ścieżki w systemie plików w menu konfiguracji agenta. Konfiguracja ścieżki musi uwzględniać wykorzystanie tzw. wildcardów (przykładowo: C\Windows\System32\dhcp\logs\Dhcp*.log – pobranie wszystkich plików z wskazanego folderu zaczynających się od "Dhcp" i kończących na ".log"), i) musi automatycznie odpytywać centralny system w zadanym interwale – tzw. heartbeat – w celu sprawdzenia czy zaszły zmiany w konfiguracji – jeżeli tak, to agent pobiera nową konfigurację, a następnie ją implementuje. Nie jest dopuszczalne "wypychanie" konfiguracji z centralnego systemu do agenta. 7. Interfejs graficzny web umożliwiający dostęp do logów, tworzenia alertów i parserów, raportów oraz zarządzania systemem musi być jednolity oraz zunifikowanym tak aby wszystkie operacje konfiguracji, zarządzania i analizy logów były w nim wykonywane. 8. Nie dopuszcza się stosowania wielu różnych interfejsów. Interfejs ten musi być dostępny z poziomu popularnych przeglądarek (przykładowo: Google Chrome, Mozilla Firefox, Opera, Microsoft Edge). 9. Stosowany w rozwiązaniu interfejs graficzny musi umożliwiać łatwe klasyfikowanie danych wejściowych (logów) na potrzeby dalszego procesowania. Klasyfikowanie powinno umożliwiać przypisywanie określonych logów do odpowiednich parserów oraz nadawanie im tagów ułatwiających dalszą pracę z logami (np. wyszukiwanie). Logika klasyfikacji powinna być tworzona przy wykorzystaniu tzw. programowania wizualnego. 10. Oferowane rozwiązanie musi umożliwiać rozbudowywanie natywnie dostępnych funkcjonalności, takich jak klasyfikacja, parsowanie, alertowanie oraz filtrowanie poprzez tak zwane programowanie wizualne, które polega

	na tworzeniu kodu z graficznych bloków reprezentujących określone instrukcje i funkcje na zasadach WYSIWYG. 11. Zamawiający wymaga, aby programowanie wizualne było możliwe do wykonania przez osoby posiadające podstawową wiedzę programistyczną taką jak znajomość min. instrukcji warunkowych, pętli czy zmiennych, jednakże rozwiązanie musi posiadać możliwość testowania i weryfikowania poprawności logiki stworzonego kodu. 12. Oferowane rozwiązanie musi udostępniać pre-definiowane widoki danych (dashboards) podzielone na kategorie pod względem typu lub producenta urządzenia źródłowego lub aplikacji. 13. Wraz z każdą nową wersją oprogramowania zapisane widoki muszą być automatycznie aktualizowane. 14. Wymagania ogólne wobec rozwiązania: a) filtrowanie nieistotnych zdarzeń na etapie klasyfikacji. Logika filtrowania powinna być tworzona przy wykorzystaniu tzw. programowania wizualnego. Wymagane jest dostarczenie dokumentacji opisującej ten proces., b) zapis oryginalnej wersji odbieranych logów, c) proste wyszukiwanie zapisanych w bazie logów i tworzenie raportów w formie graficznej bez konieczności wykorzystania dedykowanego języka programowania lub zapytań SQL. Wyszukiwanie i raporty muszą być integralną częścią oferowanego rozwiązania i muszą być dostępne przez interfejs graficzny web., d) nie dopuszcza się możliwości modyfikacji bądź manualnego usunięcia logów zapisanych w bazie. Każdy log musi posiadać unikalny identyfikator, który umożliwi jego jednoznaczne rozróżnienie., e) prezentowanie logów ma być realizowane w formie wykresów, zgrupowanych w tzw. widokach (dashboard). Widoki muszą być dynamicznie aktualizowane i interaktywne (tzw. "drill down" – przykładowo: wybranie wartości przedstawionej na jednym wykresie powoduje automatyczne utworzenie filtru wyszukiwania w oparciu o wybraną wartość i dostosowanie pozostałych wykresów)., f) tworzenie własnych parserów logów przy wykorzystaniu programowania wizualnego z poziomu interfejsu graficznego web. Wymagane jest dostarczenie dokumentacji zawierającej czytelną instrukcję tworzenia parserów., g) odbieranie wszystkich rodzajów logów. W przypadku braku odpowiedniego parsera dla odbieranego logu, system powinien zapisać go w bazie danych w formie źródłowej (RAW) i umożliwić jego wyszukiwanie., h) automatyczne wzbogacanie logi o tzw. metadane czyli informacje opisujące dany log (przykładowo: typ źródła, protokół transportowy, port docelowy, tagi, nagłówek syslog) i możliwość wyszukiwania wszystkich zapisanych logów w oparciu o te dane. Metadane powinny być dodawane do logu automatycznie nawet jeżeli nie został on poddany parsowaniu., i) musi posiadać wsparcie dla oprogramowania Elastic Beats – innymi słowy system musi umożliwiać zbieranie logów wysyłanych przez agenty Beats (filebeat/winlogbeat/auditbeat/metricbeat itd). 15. W zakresie parsowania musi być możliwość: a) tworzenia lub modyfikacji parsera – musi istnieć możliwość weryfikacji poprawności utworzonej logiki poprzez zastosowanie jej do przykładowego logu i wyświetlenie ostatecznej wersji w jakiej log zostanie zapisany w bazie, jeżeli testowany parser zostanie użyty. W przypadku wystąpienia błędów w logice parsera, system powinien poinformować o tym użytkownika., b) w procesie parsowania oferowane rozwiązanie musi normalizować odbierane

	logi do ujednoliconego formatu poprzez przypisanie poszczególnych wartości logu do odpowiadających im kluczy (format klucz = wartość). Każdy z utworzonych w procesie parsowania kluczy powinien być oddzielnie indeksowany w bazie danych aby umożliwić szybkie wyszukiwanie wartości skojarzonych z danym kluczem. Zintegrowane w systemie parsery powinny automatycznie wzbogacać procesowane logi o odpowiednią kategorię. Wymagane jest rozróżnianie przynajmniej następujących typów logów: udane logowanie, nieudane logowanie, wylogowanie, zmiana konfiguracji., c) dodania w/w kategorii podczas tworzenia własnych parserów, d) zamiany wybranych elementów logu na podstawowe typy (integer, float), w celu wykonywania na nich operacji matematycznych (suma, średnia, największa/najmniejsza wartość etc.) podczas prezentowania ich na dashboardach, e) wykorzystania operacji matematycznych (dodawanie, odejmowanie, mnożenie, dzielenie) oraz operacji natywnego kodowania/dekodowania URL. Te operacje muszą umożliwiać tworzenie logiki mającej na celu tworzenie linków URL do zewnętrznych systemów oraz połączenie narzędzia z zewnętrznymi aplikacjami., f) dodawania własnych znaczników czasu do odbieranych logów i wykorzystywać go podczas przeglądania danych. Jednocześnie system musi zachowywać oryginalny znacznik czasu z odebranych logów., g) tworzenie własnych parserów musi umożliwiać ustawienie typu wartości jako adres MAC i identyfikację producenta urządzenia sieciowego, h) automatycznego wzbogacania wartości IP wyekstraktowane z pól logu o powiązany rekord DNS i dane GeoIP aby umożliwić ich graficzną reprezentację na widoku mapy świata bez konieczności wykorzystania zewnętrznych usług bądź aplikacji, i) średnią stałą wydajność procesowania min. 2000 EPS (logów na sekundę), przy założeniu średniego rozmiaru logu równego 700 Bajtów. W przypadku wystąpienia większej chwilowej ilości logów na sekundę, rozwiązanie musi być w stanie wykorzystać bufor i umożliwić odbieranie dwukrotnej większej wartości prze co najmniej 5 minut. 16. Oferowane rozwiązanie musi umożliwiać również: a) zbieranie logów i zdarzeń z systemów Windows poprzez dedykowanego agenta instalowanego na stacji końcowej/serwerze. Agent musi być centralnie zarządzany z konsoli systemu., b) odbieranie logów na przynajmniej 50 różnych portach UDP/TCP w celu ułatwienia rozróżnienia źródeł, c) procesowanie (kolekcjonowanie oraz parsowanie) logów z dowolnych źródeł takich jak aplikacje, systemy operacyjne oraz urządzenia sieciowe, d) zbieranie logów z platformy Office365 bez konieczności instalacji dodatkowych komponentów. Proszę dostarczyć dokumentację opisującą proces konfiguracji connectora Office365., e) monitorowanie źródeł logów i tworzenie reguł mających na celu powiadamianie administratora systemu w przypadku w którym źródło logów zdefiniowane w regule nie wyśle logów w określonym interwale. System musi być dostarczony wraz z parserami do obsługi logów generowanych przez urządzenia najpopularniejszych dostawców rozwiązań IT oraz umożliwiać tworzenie własnej logiki parsowania dla nietypowych źródeł., f) odbieranie i procesowanie logów, zdarzeń oraz innych danych przesyłanych przez urządzenia w sposób jawny i ustandaryzowany, wykorzystując co najmniej następujące protokoły: UDP/TCP SYSLOG, TCP RELP (nieszyfrowany), TCP

	RELP (szyfrowany), g) łatwe tworzenie ról definiujących poziom dostępu użytkowników do zapisanych logów oraz poszczególnych elementów systemu. Wymagane jest dostarczenie dokumentacji opisującej sposób tworzenia ról użytkowników., h) wzbogacanie logów o dodatkowe informacje z zewnętrznych list (przykład: wzbogacenie nazwy użytkownika o jego adres email i przynależność do grup AD), i) integrację z systemem LDAP w celu logowania użytkowników. W przypadku awarii systemu LDAP, Zamawiający wymaga również możliwości logowania lokalnego., j) tagowanie indywidualnych źródeł danych, aplikacji, urządzeń czy całych podsieci IP, w celu oznaczania, przykładowo: lokalizacji urządzenia, jego typu, krytyczności etc. Tagi muszą być możliwe do dodania w procesie tworzenia parsera. Wszystkie dodane tagi muszą być przechowywane razem z logiem zapisanym w bazie. System musi umożliwiać filtrowanie i wyszukiwanie logów w oparciu o tagi, a także umożliwiać ograniczenie widoczności logów posiadających określony tag w procesie definiowania ról., k) wykorzystanie REST-API do integracji z zewnętrznymi systemami do monitoringu (Zabbix, Nagios, MRTG etc.), l) integrację z bazami danych (przynajmniej: MSSQL, MySQL, Oracle i PostgreSQL) poprzez konektor ODBC (integracja rozumiana jako możliwości pobierania całych wierszy wybranych tabel w bazie), m) integrację z platformą wirtualizacji Vmware (ESXi, vSphere) poprzez dedykowany konektor pobierający logi i zdarzenia bezpośrednio z platformy, n) weryfikację poprawności działania własnych parserów w trakcie ich pisania, o) zbieranie danych przynajmniej w formatach RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259, p) wspieranie podstawowych funkcji SIEM – tworzenie tzw. korelacji zdarzeń, umożliwiających wygenerowanie alertu w przypadku przekroczenia określonego limitu lub wystąpienia kilku zdarzeń w zdefiniowanym oknie czasowym. Tworzenie i edycja reguł korelacji musi być możliwa do przeprowadzenia za pomocą interfejsu programowania graficznego wyposażonego w funkcjonalność sprawdzania działania logiki reguły na przykładowych logach., q) wdrożenie w trybie wysokiej dostępności, w którym możliwe jest klastrowanie przynajmniej 2 urządzeń. Ustawienia klastra muszą być możliwe do skonfigurowania przez interfejs graficzny web, nie jest dopuszczalne konfigurowanie klastra poprzez ręczne modyfikowanie plików systemu operacyjnego. System musi dostarczać użytkownikom czytelnych informacji o stanie klastra i synchronizacji bazy. Wymaga się dostarczenia dokumentacji opisującej cały proces tworzenia klastra, oraz odzyskiwania danych w przypadku awarii jednego z komponentów klastra. Urządzenia pracujące w klastrze muszą przyśpieszać wyszukiwanie poprzez równoległe współdzielenie obciążenia., r) generowanie alertów, jeżeli w procesowanym logu zostaną spełnione zdefiniowane warunki. Alert musi być możliwy do wysłania poprzez wiadomość e-mail, a jego treść możliwa do utworzenia przez użytkownika. Oferowane rozwiązanie musi być również wyposażone w alerty i korelacje utworzone przez producenta., s) wykorzystanie pól procesowanego logu do tworzenia treści wiadomość e-mail, t) umożliwiać tworzenie alertów i korelacji poprzez wykorzystanie programowania wizualnego. Podobnie jak w przypadku tworzenia parserów, musi istnieć możliwość weryfikacji poprawności utworzonej logiki poprzez wykorzystanie testowego logu w oknie tworzenia alertu oraz powiadamiania o ewentualnych

	błędach. Wymagane jest dostarczenie dokumentacji opisującej proces tworzenia i testowania poprawności alertu., u) wysłanie logu naruszającego zdefiniowaną logikę alertu do zewnętrznych systemów, co najmniej za pomocą protokołu SMPT lub Syslog (TCP). System musi umożliwiać definiowanie własnego formatu przesyłanego logu w celu łatwiejszego dostosowania go (integracji) do systemu docelowego., v) nadawanie alertom nowych tagów, w) wspierać tworzenie i odzyskiwanie kopii zapasowej konfiguracji, x) tworzenie i odzyskiwanie kopii zapasowej bazy danych. Tworzenie kopii zapasowej musi być możliwe zarówno na żądanie jak i w określonych interwałach czasowych. Tworzenie i odzyskiwanie musi być możliwe do wykonania z poziomu interfejsu graficznego web, bez konieczności tworzenia/modyfikowania skryptów, makr lub plików systemu operacyjnego. 17. Oferowane rozwiązanie musi być dostarczone w formie urządzenia fizycznego spełniającego następujące wymagania: a) obudowa – rozmiar max 2U, wyposażone w ramię do kabli umożliwiające wysunięcie urządzenia z szafy rack na potrzeby serwisowe bez konieczności wyłączania. Wentylatory urządzenia muszą być wymienialne w trakcie pracy urządzenia i być redundantne skierowane ruchem przepływu powietrza front -> tył, b) interfejsy sieciowe – minimum 4 porty 1Gbit LAN + 1 dedykowany 1Gbit porty do zarządzania sprzętem. Konfiguracja parametrów wszystkich interfejsów sieciowych (w tym LACP) musi odbywać się z interfejsu graficznego web oraz musi być szczegółowo opisana w dokumentacji., c) zasilanie – urządzenie musi być wyposażone w 2 źródła zasilania z redundancją 1+1, d) przestrzeń dyskowa - wspierana przez sprzętowy akcelerator SAS RAID-5. Kontroler macierzy dyskowej musi być wyposażony w zapasową baterię lub pamięć flash. Minimum 4 dyski edycji RAID do wykorzystania w warunkach data center. Redundancja dysków nie może wpływać na wymaganą minimalną przestrzeń dyskową. Wymagana przestrzeń składowania danych o rozmiarze przynamniej – 12 TB oraz wspierać kompresję przechowywanych danych., e) system operacyjny - zamknięty przez producenta bez możliwości połączeń SSH. Aktualizowany z konsoli administracyjnej poprzez protokół https (wszystkie elementy systemu muszą być ustawialne z interfejsu graficznego web, bez konieczności edytowania żadnych plików systemowych, skrytpów lub makr)., f) Virtual KVM (keyboard, video, mouse) – urządzenie musi posiadać możliwość zdalnego zarządzania oraz być dostarczone z licencją odpowiedniego typu (iLO, iDRAC etc). 18. Zamawiający wymaga aby oferowane rozwiązanie gwarantowało przechowywanie danych w okresie oczekiwanej retencji aby dane były dostępne do przeszukiwania natychmiastowo, bez wprowadzania opóźnienia w postaci importu z zewnętrznych baz danych. 19. W przypadku przeciążenia systemu logi nie mogą być tracone. Wszystkie nieobsłużone logi muszą być buforowane, a administrator systemu powiadamiany w momencie, w którym bufor zacznie się zapełniać. Bufor nie może być mniejszy nić 50GB. 20. Wykonawca w momencie dostawy przekaże kompletną dokumentację – instrukcję obsługi oferowanego rozwiązania, broszurę szczegółowo przedstawiającą parametry techniczne oferowanego systemu, dokumentację w formie elektronicznej lub linku do jej wersji online na stronach producenta. Nie dopuszcza się dokumentacji odnoszącej się z/do źródeł zewnętrznych, innych

	niż producenta. 21. Zamawiający wymaga możliwości aktualizacji systemu dystrybuowanej w formie pojedynczego pliku i instalowane za pośrednictwem interfejsu graficznego web. Wszystkie aktualizacje muszą być możliwe do zainstalowania bez wsparcia dostawcy/producenta. 22. System musi umożliwiać cofnięcie do poprzedniej wersji oprogramowania w przypadku wystąpienia problemów z działaniem po aktualizacji. Operacja musi być możliwa do wykonania bez wsparcia dostawcy/producenta. 23. Ilość urządzeń z których zbierane są dane oraz ilość logów liczona w GB/dzień nie może być ograniczona licencyjnie. 24. Wymagane wsparcie na oprogramowanie – minimum 1 rok. Wymagane wsparcie na sprzęt – 5 lat. 25. Dostarczone rozwiązanie musi zostać dostarczone na koszt wykonawcy oraz uruchomione, a personel IT Zamawiającego musi zostać przeszkolony z jego obsługi. Podczas szkolenia wymaga się uruchomienia co najmniej: – 5 źródeł z systemów Microsoft Windows przykładowo: serwer MS SQL, serwer Exchange, serwer DHCP, serwer NPS, serwer Active Direcotry; – 10 źródeł urządzeń przekazujących logi poprzez syslog UDP 514 przykładowo. Apache, Cisco, Dell iDrac, FreeRADIUS, HPE iLo,BIND, Linux, Mikrotik, Nginx, OpenSSH server, PostgreSQL, Sophos, SpamAssasin, Squid, Synology NAS. 26. Rozwiązanie musi wspierać mechanizm logów o stanie alarmowym do innego systemu w formacie syslog.
Certyfikaty	Urządzenie musi posiadać deklarację CE.
Inne	Dostarczony sprzęt musi być fabrycznie nowy, sprawny technicznie, kompletny, gotowy do pracy. Wraz z dostawą musi zostać dostarczony niezbędny zestaw do zamontowania serwerów na wysuwanych szynach w szafie dystrybucyjnej 19” w tym m. in., kable zasilające, logiczne, elementy stałe, itp.
Gwarancja i wsparcie techniczne oraz serwis	60 miesięcy gwarancji i serwisu producenta lub dostawcy realizowanej w miejscu instalacji sprzętu w dniach roboczych w godzinach 8.00-15.30 z czasem naprawy do 24 godzin od przyjęcia zgłoszenia. Pod pojęciem naprawa rozumie się doprowadzenie stanu technicznego serwera do takiego samego jak sprzed awarii.

CZĘŚĆ VIII – OPROGRAMOWANIE DO ZARZĄDZANIA HASŁAMI

1. Oprogramowanie typu PAM – 1 szt.

Minimalne parametry funkcjonalne
1. Dostarczenie Systemu i przeniesienie własności na urządzenia oraz gwarancje, udostępnienia licencji niezbędnych do uruchomienia Systemu. Opracowanie projektu wdrożeniowego obejmującego instalację i konfigurację Systemu oraz integrację z oprogramowaniem/sprzętem aktualnie działającym w środowisku Zamawiającego, uruchomienie i skonfigurowanie wszystkich wymaganych urządzeń i oprogramowania w oparciu o wstępny projekt wdrożeniowy oraz przygotowanie dokumentacji post-technicznej. Przeprowadzenia szkolenia pracowników w zakresie zarządzania, administrowania i działania w ramach dostarczonego Systemu. Udzielenia 24-miesięcznej gwarancji, zgodnie z którą Dostawca/Wykonawca musi zapewnić wsparcie techniczne i serwis dla dostarczonego i aktywnego produktu. Zapewnienia pomocy technicznej eksperta. 2. Specyfikacja funkcjonalna rozwiązania: 2.1 Maszyny wirtualne – rozwiązanie, które powinno obejmować oprogramowanie działające na maszynach wirtualnych. Zamawiający zapewni zasoby niezbędne do uruchomienia maszyn

wirtualnych.
2.2 Rozwiązanie All-In-One – nie wymaga integracji z żadnym z istniejących elementów infrastruktury sieciowej (nie obejmuje implementacji w warstwach 2 i 3 modelu OSI) ani zakupu dodatkowych licencji.
2.3 Rozwiązanie umożliwia rejestrację i zarządzanie procesem dostępu uprzywilejowanego za pomocą protokołów opisanych poniżej, do 20 serwerów, gdzie serwer rozumiany jest jako unikalny adres IP z określonym protokołem komunikacyjnym.
2.4 Rozwiązanie składa się z co najmniej następujących modułów:
- Moduł zarządzania sesjami uprzywilejowanymi i rejestracji – funkcjonalność Manager Sesji,
- Moduł zarządzania hasłami dla kont na zdefiniowanych serwerach – min. dla systemów Windows, Windows Server i Unix (Linux Red Hat, Linux Suse, Linux Debian, Linux Ubuntu, FreeBSD 10+) oraz urządzeń sieciowych Cisco i baz danych MySQL – funkcjonalność Managera Haseł,
- Moduł do raportowania aktywności i przeglądu wydajności w ramach zarejestrowanych sesji,
- Moduł do zarządzania i przekazywania haseł do aplikacji – Funkcjonalność Application to Application Password Management (AAPM).

3. Szczegółowy opis wymienionych modułów (w tym AAPM):
3.1 Rozwiązanie nie powinno wymagać instalacji dodatkowego oprogramowania (agentów) ani na monitorowanych serwerach, ani na stacjach klienckich, z których będą wykonywane połączenia.
3.2 Rozwiązanie powinno posiadać mechanizmy analizy behawioralnej, które będą automatycznie wykrywać anomalie w sesjach uprzywilejowanych, zbudowane na podstawie zachowań użytkowników i indywidualnych wzorców składniowych.
3.3 Rozwiązanie pozwala na monitorowanie i rejestrację następujących protokołów:
3.3.1 Dla protokołów graficznych:
a) RDP – w tym sesje wielomonitorowe,
b) VNC.
3.3.2 Dla protokołów tekstowych:
a) SSH (w tym funkcja Proxy Jump),
b) Telnet – podwójne uwierzytelnianie dozwolone (ograniczenie protokołu).
3.3.3 W ramach aplikacji:
a) HTTP / HTTPS,
b) MySQL,
c) MS SQL i inne oparte na złączu TDS.
3.3.4 Inny:
a) systemy automatyki przemysłowej (SCADA) – min. protokół MODBUS,
b) żądany protokół TCP – dozwolona jest tylko rejestracja sesji w formacie PCAP,
c) Protokoły HTTP / HTTPS.
3.4 W zakresie protokołu RDP rozwiązanie musi wspierać połączenie z wykorzystaniem:
3.4.1 Sesje z szyfrowania TLS
3.4.2 Sesje TLS z uwierzytelnianiem NLA
3.4.3 Sesje nieszyfrowane
3.4.4 Za pomocą wbudowanego klienta (z poziomu przeglądarki internetowej)
3.5 W zakresie protokołu SSH rozwiązanie musi oferować:
3.5.1 Obsługę podsystemu SFTP - przeglądanie i pobieranie przesyłanych plików
3.5.2 Obsługa tuneli X11
3.5.3 Obsługa przekazywania tunelu agenta SSH
3.5.4 Za pomocą wbudowanego klienta (z poziomu przeglądarki internetowej)
3.6 W odniesieniu do protokołu HTTP / HTTP, wymagana jest pełna graficzna reprezentacja sesji, czyli rejestracja wszystkich elementów na stronie internetowej wraz z możliwością odtworzenia sesji w formie filmu, przedstawiającego prawdziwą stronę internetową (bez konieczności korzystania

z dodatkowej stacji przesiadkowej).

3.7 Rozwiązanie musi umożliwiać zainicjowanie sesji na dwa sposoby; poprzez wywołanie połączenia z poziomu aplikacji natywnej za pośrednictwem określonego protokołu oraz z poziomu przeglądarki internetowej, bezpośrednio poprzez stronę internetową, uruchamiając nowe połączenie z danym protokołem – przynajmniej dla protokołów RDP (rdp: //) i SSH (ssh://)

3.7.1 Funkcja uruchamiania sesji za pośrednictwem przeglądarki internetowej musi być dostępna tylko dla użytkowników, którzy zostali odpowiednio uwierzytelnieni przed wejściem na stronę główną, z której będzie prowadzone połączenie. Wspomniane uwierzytelnianie musi być również możliwe dla użytkowników zdefiniowanych w katalogu zewnętrznym – co najmniej Active Directory, LDAP i Radius

3.8 Rozwiązanie pozwala na przeglądanie i zarządzanie sesjami na żywo m.in.: wszystkimi niedokończonymi sesjami:

3.8.1 W ramach procedury, wyznaczony użytkownik musi mieć możliwość dołączenia do sesji – przynajmniej w przypadku protokołów RDP, VNC, SSH i telnet – w celu dokonania przeglądu bieżących działań

3.8.2 W rozwiązaniu musi istnieć możliwość łatwego zidentyfikowania, podmiotu aktualnie wykonującego akcje tzn.: wpisywanie znaków na klawiaturze lub używanie przycisku myszy – użytkownik inicjujący sesję lub operator dołączający do sesji

3.8.3 W rozwiązaniu musi istnieć możliwość podglądu wprowadzonych kodów/znaków wysyłanych w ramach sesji, przy czym włączenie tej funkcji nie może być możliwe bez zgody min. dwóch operatorów (użytkowników z wyższymi uprawnieniami/rolą niż zwykły użytkownik)

3.8.4 Operator przeglądający sesje na żywo, musi mieć możliwość natychmiastowego odłączenia tejże sesji i zablokowania użytkownika (poza statusem użytkownika wynikającym z synchronizacji z zasobami zewnętrznymi)

3.8.5 Operator oglądający sesję na żywo musi być w stanie zatrzymać sesję bez potrzeby odłączenia użytkownik oraz wznowienie sesji w dowolnym momencie

3.9 Administracja, monitorowanie, weryfikacja i podgląd zapisanych sesji wewnątrz rozwiązania odbywa się za pośrednictwem przeglądarki internetowej

3.10 Podgląd monitorowanych sesji, zarówno na żywo, jak i nagranych wcześniej, nie wymaga instalowania dodatkowego oprogramowania (dotyczy również wtyczek do przeglądarek, np. Flash)

3.11 W rozwiązaniu analiza i rejestracja sesji dla wyżej wymienionych protokołów będzie odbywać się wyłącznie na samym urządzeniu; nie wolno używać pomocniczych "stacji przesiadkowych"

3.12 Funkcja monitorowania sesji zapewniona przez rozwiązanie musi umożliwiać operatorowi uzyskanie informacji co najmniej o następujących zdarzeniach:

3.12.1 Rozpoczęcie sesji

3.12.2 Zakończenie sesji

3.12.3 Dołączenie do operatora lub osoby z zaproszeniem na sesję

3.12.4 Odłączenie takiego operatora lub uczestników zewnętrznych/wewnętrznych

3.13 Wyżej wymieniona funkcja musi być zaimplementowana co najmniej przy użyciu protokołu syslog i za pośrednictwem poczty elektronicznej

3.14 Rozwiązanie musi być w stanie zainicjować sesję za pomocą powiadomień z dokładnym powodem, powinno również zachować wprowadzony tekst w wewnątrz metadanych sesji

3.14.1 Dane wejściowe muszą być zaimplementowane przed ustanowieniem sesji z serwerem docelowym (systemem)

3.14.2 Wprowadzanie danych wejściowych musi być wykonywane, co najmniej dla protokołów:

a) RDP
b) VNC
c) Protokół SSH
d) telnet

3.15 Rozwiązanie pozwala kontrolować i ustawiać ograniczenia nad właściwościami sesji przy użyciu

określonych protokołów

3.15.1 Dla protokołu RDP minimum:

a) ograniczenie maksymalnej rozdzielczości ekranu sesji

b) ograniczenie głębi kolorów, min. do 8 i 16 bpp

c) blokowanie funkcji schowka

3.16 Dla protokołu SSH minimum:

a) blokowanie przekierowania portów

b) blokowanie tunelu X11

c) blokowanie przekazywania agentów SSH

d) blokowanie podsystemu SFTP i przesyłanie plików za pomocą SCP

3.17 Rozwiązanie zapewnia możliwość uwierzytelniania poprzez serwery zewnętrzne: Active Directory, Radius, LDAP (w tym OpenLDAP)

3.18 Rozwiązanie pozwala na pełną synchronizację użytkowników z Active Directory, w tym:

a) wybrane grupy w domenie Active Directory

b) dana organizacja lub dane (OU)

c) kilka domen Active Directory – również wtedy, gdy "nazwa użytkownika" jest duplikowana w dwóch domenach lub więcej

d) użytkownicy i grupy są wyodrębnione przy pomocy zdefiniowanych filtrami

3.19 Rozwiązanie rejestruje cały ruch sieciowy w odniesieniu do danej sesji (rejestracja protokołu raw)

3.20 Rozwiązanie pozwala na selektywne wskazywanie systemów, dla których nagrywanie sesji zostało pierwotnie włączone

3.21 Rozwiązanie umożliwia użytkownikowi zastąpienie loginu i hasła innym poświadczeniami określonymi na serwerze docelowym

3.22 Dla sesji graficznych rozwiązanie pozwala na uruchomienie spersonalizowanego ekranu logowania przed nawiązaniem połączenia z docelowym serwerem (systemem)

3.23 W przypadku sesji graficznych i tekstowych (przynajmniej dla protokołów SSH i telnet) rozwiązanie musi umożliwiać połączenie z serwerem (systemem) bez znajomości nazwy domeny (FQHN), bądź też adresu IP serwera (systemu), a jedynie nazwy zdefiniowanej przez operatora; przekazywanie tych informacji może odbywać się np. w formacie "user # servername", jak również za pośrednictwem wyboru danego elementu z listy lub menu rozwijanego

3.24 Rozwiązanie ma możliwość wyegzekwowania zgody operatora przed ustanowieniem sesji

3.25 Rozwiązanie musi współpracować z systemami klasy SIEM – przynajmniej przy użyciu protokołu syslog

3.26 Rozwiązanie posiada zaimplementowane rozszerzone oznaczanie powiadomień wewnętrznych wysyłanych bezpośrednio do SIEM (tagowanie), pozwalające na ustawienie odpowiednich kategorii logów/zdarzeń w takim systemie – niedopuszczalna jest konieczność wyszukiwania komunikatów dziennika zdarzeń według słów kluczowych w celu ich kategoryzacji

3.27 Rozwiązanie pozwala na zdefiniowanie konkretnego dostępu do puli niezbędnych adresów IP wraz z podsieciami (np. maska/24) – przynajmniej dla protokołów RDP, VNC, SSH i telnet

3.28 Dla protokołu RDP – rozwiązanie musi umożliwiać dostęp do podsieci systemów VDI, wykorzystując np. Connection Broker, bez konieczności definiowania każdego systemu VDI osobno

3.29 Rozwiązanie umożliwia umieszczanie komentarzy do oglądanych sesji – w trybie live, ostatnio utworzonych i wcześniej zapisanych nagrań – podczas odtwarzania

3.30 Rozwiązanie umożliwia automatyczne zakończenie sesji po wykryciu predefiniowanego ciągu znaków oraz generowanie notyfikacji do administratora

3.31 Rozwiązanie umożliwia dodatkowe zatwierdzenie połączenia uprzywilejowanego przez przełożonego (stronę trzecią) po prawidłowym uwierzytelnieniu użytkownika

3.32 Akceptacja i/lub odrzucenie sesji uprzywilejowanej przez przełożonego (funkcja wymaga zatwierdzania w ramach Bezpiecznej konfiguracji) jest również możliwa za pomocą dedykowanej aplikacji dostępnej na urządzenia mobilne

3.33 Rozwiązanie umożliwia funkcję Just-in-Time (JIT) - dostęp do zasobów poprzez żądania, gdzie system rozróżnia dwa typy zapytań dostępnych dla użytkownika:

3.33.1 natychmiastowe – żądania można ustawić od teraz i będzie ono aktywne przez np.: następne 2, 4, 6, 12 lub 24 godziny.

3.33.2 zaplanowane - użytkownik wybiera datę rozpoczęcia i datę zakończenia, co oznacza, że dostęp zostanie przyznany na cały okres od daty rozpoczęcia do daty zakończenia.

3.34 Rozwiązanie posiada funkcje przeszukiwania (skanowanie) kontrolerów domeny w celu wyodrębnienia kont o różnych poziomach uprawnień (automatyczne wykrywanie) i dodanie ich do odpowiednich sejfów i/lub gniazd zasłuchiwania.

3.35 Funkcja automatycznego wykrywania (odnajdowania) wykonuje skanowanie Active Directory tylko przy użyciu połączenia LDAP i obsługuje ją w dwóch trybach:

3.35.1 wdrażanie (onboarding) – proces, podczas którego rozwiązaniem będzie udzielanie odkrytym kontom dostępu do połączeń,

3.35.2 kwarantanna – funkcja może wysłać niezaufane konta do kwarantanny i zablokować je na serwerze docelowym

3.36 Rozwiązanie umożliwia wyszukiwanie sesji w trybie pełnotekstowym

3.37 Wyszukiwanie musi być możliwe w równym stopniu dla kanału wejściowego (np. wpisywanych poleceń) jak również dla danych wyjściowych pojawiających się na ekranie trawiącej sesji

3.38 Powyższe zapisy dotyczą w równym stopniu sesji graficznych dla protokołów RDP i VNC, i określaj całość treści pojawiających się na ekranie

3.39 Możliwość wyszukiwania musi być natychmiastowa, z wyjątkiem sesji graficznych, w których można wykorzystać silnik indeksujący OCR

3.40 Mechanizm OCR musi być zaimplementowany co najmniej dla sesji HTTP/HTTPS (zarówno dla formy tekstowej, jak i graficznej), VNC i RDP poprzez rozpoznawanie i zapisywanie we wszystkich znakach i tekstach, które były wyświetlane w ramach sesji w głównej bazie danych; dotyczy to zarówno tekstów (poleceń) wprowadzanych na klawiaturze, jak i znaków/fraz, które pojawiły się w dowolnym miejscu na ekranie sesji graficznej (okna aplikacji, dane edytowanych dokumentów, "wyskakujące" okna powiadomień, nazwy plików itp.)

3.41 Przygotowanie sesji do weryfikacji musi odbywać się wewnętrznie, tzn. dane nie mogą być przesyłane do chmury lub innego dedykowanego urządzenia

3.42 Funkcja wyszukiwania musi być wyłączona co najmniej na poziomie określonego użytkownika na serwerze

3.43 Rozwiązanie pozwala na przyznanie czasowego dostępu do pojedynczej sesji – zarówno w zakresie zakończonej i zapisanej, jak i niedokończonej ("live")

3.43.1 W ramach sesji niedokończonej ("live"), operator musi mieć możliwość określenia, czy sesja ma być udostępniana tylko w trybie podglądu, czy też z opcją dołączenia/udostępnienia sesji uczestnikom zewnętrznym

3.43.2 Musi istnieć możliwość cofnięcia udzielonego dostępu do wspólnej sesji w dowolnym momencie

3.44 Rozwiązanie posiada możliwość monitorowania, raportowania i analizowania aktywności/efektywności użytkowników podczas sesji, z uwzględnieniem modułu analizy biznesowej

3.44.1 Analiza sesji powinna szczegółowo przedstawiać, w jaki sposób produktywność użytkowników / organizacji rozwijała się w każdym okresie.

3.44.2 Konfigurowalny parametr definiujący próg aktywności powinien pozwolić na szybką identyfikację sesji, użytkowników lub organizacji, które nie przekroczyły wymaganego poziomu aktywności, a także wspomóc proces wskazywania wartości progowej, przy której dana liczba użytkowników lub sesji osiąga wymagany poziom aktywności.

3.44.3 Musi istnieć możliwość określenia aktywności sesji w skali 0% - 100%, wynikającej z liczby zarejestrowanych zdarzeń wejściowych (wysłany kod klucza, a dla sesji graficznych każde użycie mysz; ruch i kliknięcia przycisków funkcyjnych – jeśli dla danego protokołu rejestracja takich elementów została aktywowana)

3.44.4 Komponent analizy produktywności powinien umożliwiać porównywanie aktywności organizacji lub użytkowników w określonych odstępach czasu.

3.45 Rozwiązanie musi być w stanie zdefiniować hierarchię użytkowników i operatorów, przynajmniej pod względem:

3.45.1 konto regularnego dla użytkownika

3.45.2 konta operatora z dostępem do standardowego trybu podglądu

3.45.3 konta operatora z trybem przeglądu konfiguracji

3.45.4 konta operatora z możliwością dostosowania konfiguracji

3.45.5 konta operatora z możliwością zarządzania systemem (np. restart urządzenia)

3.46 Rozwiązanie musi być w stanie zdefiniować dostęp dla operatora co najmniej do:

3.46.1 wskazanych serwerów (systemy) oraz zapisanych i trwających sesji

3.46.2 wyznaczonych użytkowników wraz z zapisanymi i trwającymi sesjami

3.47 Rozwiązanie musi umożliwiać nałożenie znaczników czasu na nagrane sesje

3.48 Rozwiązanie musi mieć opcję zdefiniowania polityki sesji/przechowywania danych, czyli określenia okresu, po którym sesje zostaną usunięte z urządzenia

3.48.1 Musi istnieć możliwość zdefiniowania różnych czynników przechowywania sesji/danych

3.49 Rozwiązanie musi posiadać możliwość integracji z zewnętrznym repozytorium haseł firmowych:

3.49.1 CyberArk

3.49.2 Thycotic

3.49.3 LAPS

3.50 Rozwiązanie musi posiadać funkcjonalność sprawdzania hasła

3.51 Rozwiązanie musi być zintegrowane ze standardem uwierzytelniania opisanym w RFC 6287 (OATH)

3.52 Rozwiązanie musi umożliwiać zdefiniowanie zestawu poleceń lub ciągów znaków, które (wprowadzone podczas sesji lub występujące w treści sesji) wywołają akcję zdefiniowaną przez operatora, co najmniej jako:

3.52.1 informacje wysyłane za pomocą protokołu syslog

3.52.2 informacje przesyłane do systemu SIEM

3.52.3 notyfikacja operatora za pośrednictwem poczty elektronicznej

3.52.4 natychmiastowe zakończenie aktywnej sesji z dodatkową opcją automatycznego blokowania podejrzanego użytkownika, niezależnie od stanu użytkownika wynikającego z synchronizacji z zasobami zewnętrznymi

3.52.5 zatrzymanie trwającej sesji

3.53 zestaw poleceń lub ciągów wspomnianych powyżej musi być możliwy do zdefiniowania za pomocą mechanizmu wyrażeń regularnych (regexp), mechanizm symboli wieloznacznych nie będzie uważany za równoważny

3.54 wyżej opisana funkcjonalność musi być możliwa do osiągnięcia przynajmniej dla protokołów:

3.54.1 RDP

3.54.2 VNC

3.54.3 Protokół SSH

3.54.4 Telnet

3.55 Wymienione funkcje powinny rozpoznawać polecenia lub ciągi znaków w następujących przypadkach:

3.55.1 poprawne egzekwowanie reguły co najmniej dla protokołów VNC, RDP – w zakresie danych wejściowych i danych sesji dostępnych po indeksowaniu po zakończeniu sesji

3.55.2 dla innych protokołów - podczas trwającej sesji, natychmiast po rozpoznaniu danego ciągu znaków, identycznie dla danych wejściowych i wyjściowych pojawiających się na ekranie sesji

3.55.3 konfigurowanie ograniczenia tylko dla danych wejściowych/wyjściowych, które pojawiają się na ekranie nawiązanej sesji

3.56 Rozwiązanie musi posiadać opcję zapisu sesji w formie nagrania wideo (zapis liniowy)

w formacie umożliwiającym odtworzenie nagrania przy użyciu programu VLC 3.0 lub wersji najnowszej:

3.56.1 taki zapis musi być możliwy dla protokołów graficznych (co najmniej VNC i RDP) i tekstowych (co najmniej SSH i telnet)

3.57 zarządzanie skryptami rozwiązania dla udokumentowanego API musi mieć opcję co najmniej:

3.57.1 tworzenia, modyfikowania i usuwanie kont użytkowników

3.57.2 tworzenia, modyfikowania i usuwanie serwerów (systemów docelowych)

3.57.3 tworzenia, modyfikowania i usuwanie dostępu do serwerów (systemów) – w odniesieniu do kont

3.57.4 tworzenia, modyfikowania i usuwanie adresów IP i portów, z którymi użytkownicy będą się łączyć

3.57.5 tworzenia, modyfikowania i usuwanie relacji między kontami, serwerami, czy poszczególnymi dostępami

3.57.6 pobieranie listy sesji – z możliwością wyróżnienia sesji, które nie zostały jeszcze zakończone

3.57.7 blokowanie użytkownika – niezależnie od stanu synchronizacji użytkownika pod kątem zasobów zewnętrznych

3.58 rozwiązanie musi pozwalać na odzyskiwanie systemu co najmniej do poprzedniej wersji po wadliwej aktualizacji

3.59 funkcja ta musi być dostępna bezpośrednio z poziomu interfejsu zarządzania, bez konieczności korzystania z wiersza poleceń lub dedykowanej konsoli zarządzania (terminala)

4. Szczegółowa specyfikacja modułu zarządzania hasłami

4.1 Rozwiązanie musi obsługiwać funkcję zmiany haseł w systemach Unix przy użyciu uprzywilejowanego konta z dostępem za pomocą klucza SSH

4.2 Rozwiązanie umożliwia definiowanie sekwencji poleceń wyzwalających modyfikację hasła

4.3 Rozwiązanie umożliwia weryfikację czy hasło nie zostało zmienione w sposób nieautoryzowany

4.4 Rozwiązanie przechowuje historię hasła do konta i ma możliwość odzyskania wybranego hasła

4.5 Rozwiązanie pozwala zdefiniować złożoność automatycznie generowanych haseł

5. Specyfikacja modułu zarządzania hasłami i mechanizmu przekazywania

5.1 Rozwiązanie zapewnia bezpieczną wymianę haseł pomiędzy aplikacjami – funkcjonalność AAPM

5.2 Autoryzacja dostępu do danych w systemie AAPM powinna opierać się na adresie IP oraz jednorazowym lub statycznym haśle

5.3 Moduł musi współpracować przynajmniej z oprogramowaniem, które działa pod kontrolą systemu operacyjnego:

a) Windows Server 2012 lub nowszy

b) Linux – Red Hat 6 lub nowszy (lub równoważna, ale nie starsza, inna dystrybucja)

c) FreeBSD 10 lub nowszy

6. Specyfikacja techniczna

6.1 Rozwiązanie zapewnia kryptograficzną ochronę wszystkich zapisanych danych (szyfrowanie i integralność) na poziomie bezpieczeństwa nie niższym niż poziom gwarantowany przez kod AES 256

6.1.1 Dostawca/producent rozwiązania nie powinien mieć możliwości odszyfrowania jakichkolwiek danych przechowywanych na urządzeniu bez dostępu do oryginalnych kluczy szyfrujących (brak kluczy serwisowych)

6.1.2 Kryptograficzna ochrona przechowywanych danych musi być realizowana co najmniej na poziomie bazy danych (dane są szyfrowane wewnątrz bazy), a także na poziomie nośnika, na którym działa system (szyfrowanie całego systemu plików, również dla instalacji wirtualnej), a funkcja szyfrowania nośników musi być integralną częścią rozwiązania

6.2 Rozwiązanie posiada możliwość konfiguracji klastra:

6.2.1 minimalna liczba węzłów w klastrze: 2

6.2.2 Musi istnieć możliwość świadczenia usług w trybie wysokiej dostępności przy użyciu

wirtualnego ("pływającego") adresu IP
6.3 Rozwiązanie nie może pracować w trybie "hot standby", tzn. wszystkie węzły klastra muszą aktywnie uczestniczyć we wdrażaniu funkcjonalności rozwiązania, zgodnie ze zdefiniowaną polityką, np.: musi istnieć możliwość określenia, który węzeł klastra będzie obsługiwał dany zestaw sesji
6.4 musi istnieć możliwość ręcznej zmiany roli węzła w klastrze, np. przeniesienia funkcjonalności z węzła, który ma zostać przeniesiony lub modyfikacja węzła w obrębie instancji
6.5 Rozwiązanie posiada zarezerwowaną przestrzeń dyskową na dane (użytkową) pozwalającą na rejestrację i przechowywanie zebranych danych (monitorowanych sesji) przez minimalny okres (ustalony osobno dla każdej pojemności pamięci urządzenia) – 180 dni dla sesji RDP, przy założeniu przechowywania minimum 50 sesji RDP dziennie, gdzie jedna sesja trwa średnio 8 godzin. A szacowany rozmiar pojedynczej sesji jest równy, średnio 300 MB.
6.6 rozwiązanie musi dysponować wystarczającą ilością pamięci masowej, która pozwoli na jednoczesną rejestrację do min. 100 sesji tekstowych (dla protokołów SSH, telnet) lub min. 30 sesji (dla protokołów RDP, VNC) - liczonych dla pojedynczego urządzenia lub dla klastra z tylko jednym aktywnym węzłem.
6.7 urządzenie musi pracować w następującym trybie:
6.7.1 serwer, do transmisji (warstwa 5+ modelu OSI)
6.7.2 aplikacja – nasłuchiwanie na wskazanym adresie IP/adresach i portach
6.7.3 tryb routera (brama, warstwa 3 modelu OSI) - wysyłanie pakietów/ruchu tylko do zdefiniowanych serwerów (systemów) pomiędzy dwoma segmentami sieci IP
6.7.4 tryb mostka (warstwa 2 modelu OSI) – wysyłanie całego ruchu sieciowego między dwoma punktami końcowymi w ramach zwykłego połączenia Ethernet, ale nie może zakłócać pakietów, które nie są częścią ruchu sieciowego należącego do sesji i będących w równym stopniu obsługiwanymi przez urządzenie
6.8 Rozwiązanie musi umożliwiać zdefiniowanie własnego certyfikatu/klucza dla połączeń szyfrowanych (dla protokołów RDP i SSH) oraz przeniesienie istniejących certyfikatów/klucza z serwera (systemu), do którego zdefiniowany jest dostęp - obsługa fraz szyfrujących certyfikat/klucz
6.9 Rozwiązanie musi umożliwiać weryfikację certyfikatu/klucza serwera (systemu), do którego zdefiniowany jest dostęp – przynajmniej dla protokołów RDP i SSH
6.9.1 W przypadku protokołu RDP musi istnieć możliwość weryfikacji certyfikatu serwera docelowego (systemu) na podstawie zdefiniowanego początkowo certyfikatu CA (zaimportowanego)
6.10 Rozwiązanie obsługuje pakiety oznaczone zgodnie ze standardem 801.1q (VLAN)
6.11 Rozwiązanie obsługuje agregację 802.3ad (LACP) dla każdego typu interfejsu sieciowego – tj. zarówno dla interfejsów używanych do nasłuchiwania, interfejsu przesyłania danych (interfejsów), jak i interfejsu zarządzania
6.12 Rozwiązanie musi mieć możliwość monitorowania wybranych parametrów pracy za pomocą protokołu SNMP, wersja min. v3
6.13 Rozwiązanie musi umożliwiać podstawową diagnostykę sieci:
6.14 Potwierdzenie komunikacji za pomocą sygnalizacji ICMP (ping)
6.14.1 potwierdzenie komunikacji za pomocą połączenia TCP (połączenie z dowolnym portem o dowolnym adresie IP)
6.15 Rozwiązanie musi współpracować z następującymi usługami sieciowymi:
6.15.1 NTP
6.15.2 serwer nazw (DNS)
6.16 Rozwiązanie obsługuje polską klawiaturę (programistę)
6.17 Rozwiązanie posiada dokumentację oraz interfejs użytkownika w języku polskim i angielskim
6.18 Rozwiązanie posiada wsparcie techniczne w języku polskim i angielskim
7. Specyfikacja obsługi rozwiązania
7.1 Wsparcie dla rozwiązania musi być aktywne – tj. w ciągu ostatnich 2 kwartałów od daty końcowego wdrożenia, rozwiązanie otrzymało min. 3 aktualizacje (pakiety takie jak: aktualizacja

wersji głównej, wydanie pomocnicze, poprawki błędów, hot patche)

7.2 Rozwiązanie musi zawierać wszystkie niezbędne licencje do uruchomienia powyższych funkcjonalności, w tym licencje systemu operacyjnego - jeśli są niezbędne do jego uruchomienia

8. Specyfikacja maszyny wirtualnej

8.1 Rozwiązanie musi działać co najmniej na następujących platformach wirtualizacji:

8.1.1 VMware 5.x

8.1.2 VMware 6.x

8.1.3 KVM / OpenStack / Proxmox lub jakikolwiek inny oparty na KVM lub qemu hypervisor

8.1.4 XCP-NG 8.x

9. W ramach przedmiotowego postępowania wymagane jest dostarczenie Zamawiającemu licencji wieczystych realizujących wszystkie funkcjonalności systemu dla minimum 20 urządzeń aktywnych (serwerów) Zamawiającego.

10. Do oferowanych licencji oprogramowania należy zapewnić 2 letnie (24 miesięcy) wsparcie techniczne (Support) producenta.