

**Załącznik nr do SWZ**

**Opis przedmiotu zamówienia (OPZ)**

**Nazwa zamówienia:**

**Dostawa i sprzedaż urządzeń i oprogramowania zwiększających odporność na cyberataki**

**wraz z wdrożeniem w ramach Projektu „Cyberbezpieczny Samorząd”**

**Zamawiający:**

**Znak sprawy:**

**Spis Treści:**

1. System do zbierania i analizy logów – 1 szt.
2. System do ochrony poczty elektronicznej – 1 szt.
3. System do zarządzania siecią, infrastrukturą i użytkownikami – 80 licencji wieczystych ze wsparciem do dnia 30.06.2026
4. System NAC – 150 licencji wieczystych ze wsparciem do dnia 30.06.2026
5. Oprogramowanie Advanced Threat Protection – 90 licencji z subskrypcją.
6. Oprogramowanie antywirusowe – 100 licencji z subskrypcją do dnia 30.06.2026
7. Centralnie zarządzane switche – 9 szt.
8. Centralnie zarządzane access pointy – 5 szt.
9. System do backupu danych – 1 szt.
10. Zasilanie awaryjne – UPS – serwery – 2 szt.
11. Zasilanie awaryjne – UPS – stacje robocze – 68 szt.
12. Agregat prądotwórczy – 1 szt
13. Szkolenia z zakresu cyberbezpieczeństwa dla pracowników oraz kadry kierowniczej
14. Szkolenia specjalistyczne dla administratorów w zakresie planowanych do zastosowania środków bezpieczeństwa

# 1.

# System do zbierania i analizy logów – 1 szt.:

**Wymagania Ogólne:**

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

**Interfejsy, Dysk, Zasilanie:**

1. System musi dysponować co najmniej 2 portami Gigabit Ethernet RJ-45.
2. Rozwiązanie musi dysponować powierzchnią dyskową min. 4 TB.
3. System musi być wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. System musi być w stanie przyjmować do 25 GB logów na dzień.
2. System musi być w stanie przeanalizować do 500 logów na sekundę.
3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 50 systemów.

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

**Logowanie:**

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
4. listę najczęściej wykrywanych ataków,
5. listę najbardziej aktywnych użytkowników,
6. listę najczęściej wykorzystywanych aplikacji,
7. listę najczęściej odwiedzanych stron www,
8. listę krajów, do których nawiązywane są połączenia,
9. listę najczęściej wykorzystywanych polityk Firewall,
10. informacje o realizowanych połączeniach IPSec.
11. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania   
    i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
12. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
13. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

**Raportowanie:**

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

**Korelacja logów:**

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

* malware,
* aplikacje sieciowe,
* email,
* IPS,
* traffic,
* systemowe: utracone połączenie VPN, utracone połączenie sieciowe.

**Zarządzanie:**

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

**Gwarancja oraz wsparcie:**

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7 minimum do dnia 30.06.2026 roku.
2. Dla zapewnienia wysokiego poziomu usług, świadczenie wsparcia technicznego musi być realizowane przez wykonawcę na poziomie min. zaawansowanym, posiadającego aktywne specjalizacje:
3. w zakresie Operacji Bezpieczeństwa (SO),
4. w zakresie Dostępu Zero Trust (ZTNA),
5. w zakresie Zdefiniowanej Programowo Sieci Rozległej (SD-WAN),
6. w zakresie Bezpieczna Łączność LAN (SD-Branch),
7. w zakresie Technologii Operacyjnej (OT),
8. w zakresie Krawędzi Usługi Bezpiecznego Dostępu (SASE),
9. w zakresie Bezpieczeństwa Chmury Publicznej (Cloud).

**Rozszerzone wsparcie serwisowe:**

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesięcy.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.

**Oferent winien przedłożyć dokumenty**:

* oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej),
* certyfikat ISO 9001 podmiotu serwisującego.

**Wdrożenie:**

Od Wykonawcy wymaga się wdrożenia dostarczonego rozwiązania wraz z pełną konfiguracją i integracją z infrastrukturą informatyczną Zamawiającego.

Wdrożenie musi być przeprowadzone przez certyfikowanego inżyniera, posiadającego minimum   
4 aktywne certyfikaty producenta oferowanego w postępowaniu systemu do zbierania i analizy logów na poziomie:

* certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci (NS),
* certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej (PCS),
* certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa (SO),
* certyfikowany Specjalista w zakresie Dostępu na Krawędzi Sieci (SASE).

**Certyfikaty osobowe załączyć do oferty.**

**Opisy do wymagań ogólnych:**

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien **przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora** producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

# 2.

# System do ochrony poczty elektronicznej – 1 szt.:

**Wymagania ogólne:**

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

**Parametry fizyczne systemu antyspamowego:**

1. System musi być wyposażony w interfejsy: 4 porty Gigabit Ethernet RJ-45.
2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB.
3. System musi posiadać wbudowany port konsoli szeregowej.
4. Zasilanie z sieci 230V/50Hz.

**Ogólne funkcje systemu ochrony poczty:**

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 28 tysięcy wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika   
   i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

**Kontrola antywirusowa i ochrona przed malware:**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.

**Kontrola antyspamowa:**

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

**Ochrona przed atakami na usługę poczty:**

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

**Funkcje logowania i raportowania:**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

**Funkcje pracy w trybie wysokiej dostępności (HA):**

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

**Aktualizacje sygnatur, dostęp do bazy spamu:**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz URL uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

**Zarządzanie:**

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.

**Certyfikaty:**

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

**Serwisy i licencje:**

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

1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake na okres minimum do dnia 30.06.2026 roku.

**Gwarancja oraz wsparcie:**

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7 minimum do dnia 30.06.2026 roku.
2. Dla zapewnienia wysokiego poziomu usług, świadczenie wsparcia technicznego musi być realizowane przez wykonawcę na poziomie min. zaawansowanym, posiadającego aktywne specjalizacje:
3. w zakresie Operacji Bezpieczeństwa (SO),
4. w zakresie Dostępu Zero Trust (ZTNA),
5. w zakresie Zdefiniowanej Programowo Sieci Rozległej (SD-WAN),
6. w zakresie Bezpieczna Łączność LAN (SD-Branch),
7. w zakresie Technologii Operacyjnej (OT),
8. w zakresie Krawędzi Usługi Bezpiecznego Dostępu (SASE),
9. w zakresie Bezpieczeństwa Chmury Publicznej (Cloud).

**Rozszerzone wsparcie serwisowe:**

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesięcy.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.

**Oferent winien przedłożyć dokumenty**:

* Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
* Certyfikat ISO 9001 podmiotu serwisującego.

**Wdrożenie:**

Od Wykonawcy wymaga się wdrożenia dostarczonego rozwiązania wraz z pełną konfiguracją i integracją z infrastrukturą informatyczną Zamawiającego.

Wdrożenie musi być przeprowadzone przez certyfikowanego inżyniera, posiadającego minimum   
4 aktywne certyfikaty producenta oferowanego w postępowaniu systemu do ochrony poczty elektronicznej na poziomie:

* certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci (NS),
* certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej (PCS),
* certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa (SO),
* certyfikowany Specjalista w zakresie Dostępu na Krawędzi Sieci (SASE).

**Certyfikaty osobowe załączyć do oferty.**

**Opisy do wymagań ogólnych:**

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien **przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora** producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

# 3.

# System do zarządzania siecią, infrastrukturą i użytkownikami – 80 licencji wieczystych ze wsparciem do dnia 30.06.2026

Oprogramowanie powinno posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami powinna być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Program powinien umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą. Moduły powinny umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program powinien wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12) i nie może być objęty limitem ilości danych, a baza danych ma być rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających powinna wymagać 64-bitowego systemu operacyjnego Windows.

Dane, które dotyczą działań pracownika na komputerze (historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp.), powinny być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej i grupowane w osobnym, dedykowanym oknie. Oprogramowanie umożliwiać ma, zgodnie z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.

Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty ma być kontrolą na poziomie wybranych Administratorów – program umożliwiać ma nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator ma mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów powinny być logowane, co oznacza, że program powinien posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów powinny być automatycznie eksportowane do zewnętrznego kolektora Syslog.

Program powinien umożliwiać konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityka powinna pozwalać na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymuszać dostosowanie bieżących haseł do obowiązujących zasad.

Program zawierać powinien mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny powinien być wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA powinno dać się skonfigurować okres, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania powinna być pominięta wyłącznie w lokalnej konsoli serwera.

Wymaga się, aby producent oprogramowania posiadał znak jakości CYBERSECURITY MADE IN EUROPE, przyznany przez Europejską Organizację ds. Cyberbezpieczeństwa (ECSO).

**Oprogramowanie powinno mieć możliwość monitorowania infrastruktury (bezagentowo) obejmujące serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:**

* wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping,
* wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU),
* wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci,
* wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki,
* wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła,
* wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku,
* wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze,
* wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie,
* wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny,
* zablokowania mapy urządzeń przed przypadkową edycją,
* serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów,
* serwerów pocztowych:
  + program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem),
  + program ma możliwość wykonywania operacji testowych,
  + program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa.
* monitorowania serwerów WWW i adresów URL,
* cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS,
* obsługi szyfrowania SSL/TLS w powiadomieniach e-mail,
* obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID,
* obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych,
* monitoringu routerów i przełączników wg:
  + zmian stanu interfejsów sieciowych,
  + ruchu sieciowego,
  + podłączonych stacji roboczych – graficzna prezentacja panelu switcha,
  + ruchu generowanego przez podłączone do portów stacje robocze.
* serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie,
* wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu,
* monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano,
* zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny,
* wydajności systemów Windows:
  + obciążenie CPU,
  + obciążenie pamięci,
  + zajętość dysków,
  + transfer sieciowy.

Program powinien posiadać Inteligentne Mapy i Oddziały, służące do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzące dynamiczne mapy wg własnych filtrów (Mapy Inteligentne).

Kryteria automatycznego filtrowania dotyczyć mają m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program powinien posiadać również funkcję kompilatora plików MIB, umożliwiającego dodawanie definicji dla modułów SNMP.

Program powinien umożliwiać również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy powinny być budowane przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów powinno dać się skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji powinno dać się nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy mają pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie powinno umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0.

Program powinien mieć możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

**W zakresie inwentaryzacji program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:**

1. Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
2. Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
3. Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio będzie umożliwiać audytowanie i weryfikację użytkowania licencji w organizacji.
4. Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
5. Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
6. Umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
7. Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
8. Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
9. Umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
10. Umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji mają być logowane.

**Moduł inwentaryzacji zasobów powinien umożliwiać ma prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:**

* przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
* tworzenia powiązań między zasobami a urządzeniami,
* tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
* wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
* definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
* określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
* określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
* definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
* importu danych z zewnętrznego źródła (.CSV),
* przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
* tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
* oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
* ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
* generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
* przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
* konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
* konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
* archiwizacji i porównywania audytów zasobów,
* tworzenia kodów kreskowych dla zasobów,
* drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
* inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
* możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
* inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
* definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

**Inwentaryzacja oprogramowania powinna zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:**

1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
2. Informacje o aplikacjach używanych w organizacji.
3. Tworzenie własnych wzorców aplikacji.
4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
5. Informacje o komputerach, na których aplikacja została wykryta.
6. Zarządzanie posiadanymi licencjami.
7. Wskazywanie osób odpowiedzialnych za licencję.
8. Wskazanie użytkowników licencji.
9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili powinna być możliwość wykonania aktualnych raportów audytowych.
12. Zarządzanie posiadanymi licencjami: raport zgodności licencji.
13. Możliwość przypisania do programów numerów seryjnych, wartości itp.

Okna audytowe powinny posiadać możliwość filtrowania elementów per oddział.

**W zakresie obsługi użytkowników program powinien umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:**

* faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
* procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
* rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
* informacji o edytowanych przez użytkownika dokumentach,
* historii pracy (cykliczne zrzuty ekranowe),
* listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),
* transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
* wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Możliwość monitorowania kosztów wydruków,
* nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

**Program ponadto powinien posiadać możliwość:**

* wykrywania podejrzanej aktywności przez tzw. „jigglery”, mającej na celu symulowanie faktycznej pracy,
* zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury,
* wyszczególnienia podejrzanej aktywności w raportach,
* wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności
* automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności,
* blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl). Reguły w postaci listy domen tworzone dla użytkownika lub grupy użytkowników i kopiowane lub współdzielone pomiędzy grupami lub kontami,
* integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.,
* skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia,
* automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych,
* blokowania ruchu na wskazanych portach TCP/IP,
* blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
* prowadzenia rejestru naruszeń blokad,
* wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
* przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
* definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.

Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.

Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji powinny być tworzone dla użytkownika lub grupy użytkowników i powinny być kopiowane pomiędzy grupami lub kontami.

Program powinien posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

**Oprogramowanie powinno mieć możliwość ochrony danych przed wyciekiem poprzez blokowanie urządzeń:**

1. Blokowanie urządzeń i nośników danych. Program ma mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
9. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.
10. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
11. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
12. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

**Zarządzanie prawami dostępu do urządzeń:**

1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. - urządzenia prywatne są blokowane.
3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

**Audyt operacji na plikach na urządzeniach przenośnych:**

1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
2. Podłączenie/odłączenie urządzenia przenośnego.

Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.

Definiowanie reguł monitorowanych folderów w postaci list.

Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.)

Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.

Program umożliwiać powinien prowadzenie rejestru naruszeń blokad podłączanych nośników.

**Portal informacyjny w formie platformy WWW:**

Oprogramowanie posiadać powinno obszar funkcjonalny w formie platformy WWW, który pozwalać ma na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami. Na każdym z dashboardów widgety powinny być rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych powinna być automatycznie odświeżana oraz:

* udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem,
* wyświetlana w trybie jasnym lub ciemnym (nocnym).

Oprogramowanie umożliwiać powinno zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego.

Widgety powinny prezentować dane ze wszystkich modułów funkcjonalnych oprogramowania.

**Ochrona przed usunięciem:**

Program powinien być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.

**Funkcjonalność Agenta:**

Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.

**Inne:**

Globalna wyszukiwarka, zwracająca wyniki obiektów różnego typu na podstawie wyszukiwanych słów kluczowych, np.: urządzenia, użytkownicy, zasoby, elementy interfejsu konsoli zarządzającej, elementy opcji. Program ma być dostępny minimum w języku polskim, angielskim, wraz z Podręcznikiem Użytkownika w formie strony internetowej.

**Wdrożenie:**

Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, przeprowadzoną przez wykwalikowanego inżyniera, certyfikowanego przez producenta rozwiązania.

Wymaga się, aby dostawca przedstawił osobowy certyfikat pracownika, który będzie wykonywał wdrożenie (**certyfikat załączyć do oferty**).

Wsparcie techniczne oprogramowania powinno obowiązywać minimum do dnia 30.06.2026 roku.

# 4.

# System NAC 150 licencji wieczystych ze wsparciem do dnia 30.06.2026

**Opis funkcjonalności rozwiązania:**

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.

**Wymagania ogólne rozwiązania NAC:**

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, 150 licencji wieczystych oraz wsparcia technicznego i konserwacji na okres minimum do 30.06.2026 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.

**Wymagania szczegółowe – monitorowanie podsieci:**

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

**Wymagania szczegółowe – polityka bezpieczeństwa:**

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:
   1. pełny dostęp,
   2. blokowanie (całkowity brak dostępu),
   3. 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.

**Wymagania szczegółowe – mechanizm kwarantanny:**

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:
   1. całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym,
   2. częściowe blokowanie komunikacji urządzenia z otoczeniem sieciowym, w zakresie definiowanym przez administratora przez wskazanie adresów IP i portów, z którymi urządzenie może się komunikować.
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

**Wymagania szczegółowe – integracja z systemami zewnętrznymi:**

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, Carbon Black, CrowdStrike, Cybereason, Eset, FireEye, 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 urządzenia.

**Wymagania szczegółowe – rejestracja urządzeń zewnętrznych: pracowników, gości i konsultantów (Captive Portal):**

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 faktora, 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

**Usługi:**

Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, w wymienionym poniżej zakresie, przeprowadzoną przez wykwalikowanego inżyniera, certyfikowanego przez producenta rozwiązania:

* instalacja i konfiguracja sprzętowego appliance’a,
* szkolenie dla administratora rozwiązania,
* wsparcie w języku polskim w trybie 8x5 w dni robocze,
* kwartalny przegląd konfiguracji rozwiązania.

Wymaga się, aby dostawca przedstawił (**załączyć do oferty**):

* oświadczenie producenta o posiadaniu przez dostawcę kwalifikacji technicznych, niezbędnych do wykonania wdrożenia oferowanego rozwiązania i szkolenia,
* osobowy certyfikat inżynierski pracownika, który będzie wykonywał wdrożenie.

# 5.

# Oprogramowanie Advanced Threat Protection 90 licencji z subskrypcją do dnia 30.06.2026

**Opis funkcjonalności rozwiązania:**

Wymagane jest dostarczenie rozwiązania służącego do ochrony urządzeń końcowych przed złośliwym oprogramowaniem. Rozwiązanie musi być realizowane w postaci agenta instalowanego na urządzeniu końcowym, zarządzane przez jedną chmurową konsolę administracyjną. Wymagana jest obsługa urządzeń z systemami Windows, MacOS, Linux, Android i iOS.

Rozwiązanie musi zapewniać skuteczną ochroną zarówno przez zapobieganie uruchomieniu złośliwego kodu (funkcjonalność antymalware), jak i wykrywanie zainicjowanego ataku w jego początkowej fazie i automatyczne reagowanie (funkcjonalność EDR). Ze względu na zaawansowanie techniczne, intensywność i różnorodność obecnych cyberzagrożeń, wymaga się, aby rozwiązanie było oparte na modelach matematycznych, opracowanych z użyciem uczenia maszynowego i sztucznej inteligencji. Rozwiązanie musi być jednakowo skuteczne w trybie online, gdy urządzenie końcowe ma połączenie z chmurą, jak i w trybie offline, bez dostępu do Internetu. Agent na urządzeniu końcowym powinien działać w tle i korzystać z zasobów urządzenia (procesor, pamięć) w sposób nie wpływający na normalną pracę użytkownika.

Konfiguracja rozwiązania, wizualizacja stanu bezpieczeństwa i zarządzanie muszą być w całości wykonywane na konsoli administracyjnej.

Wymaga się dostarczenia rozwiązania z **subskrypcją licencji minimum do dnia 30.06.2026 roku**, pozwalającą objąć ochroną **90 urządzeń**.

**Wymagania szczegółowe – architektura i zarządzanie rozwiązaniem:**

1. Całość zarządzania rozwiązaniem, w tym konfiguracja sposobu działania agentów (polityki bezpieczeństwa), lista chronionych urządzeń, wizualizacja stanu bezpieczeństwa, raportowanie, badanie wykrytych incydentów, itp. musi być realizowana w jednej chmurowej konsoli administracyjnej, udostępnianej przez producenta.
2. Ochronę urządzenia końcowego musi realizować agent, instalowany na tym urządzeniu. Dopuszcza się zarówno pojedynczego agenta, jak i dwóch agentów, realizujących odpowiednio funkcje ochrony antymalware i EDR.
3. Konsola musi prezentować listę zarządzanych urządzeń, z podaniem dla każdego urządzenia jego nazwy, adresu IP, systemu operacyjnego, nazwy zalogowanego użytkownika, wersji zainstalowanego agenta, statusu online/offline, przypisanej do urządzenia polityki bezpieczeństwa, zdarzeń zarejestrowanych przez agenta.
4. Agent musi być dostępny dla systemów Windows, MacOS, Linux, Android, iOS.
5. Instalator agenta musi być dostępny do pobrania: dla urządzeń desktopowych z konsoli administracyjnej, dla urządzeń mobilnych z Google Play i Apple Store.
6. Agent musi pobierać swoją konfigurację (sposób działania) z konsoli administracyjnej. Komunikacja między agentem i konsolą musi być inicjowana przez agenta, szyfrowana protokołem TLS i korzystać wyłącznie z protokołu https na port wychodzący 443.
7. Rozwiązanie musi zapewniać, że zainstalowany agent komunikuje się i współpracuje wyłącznie z konsolą administracyjną danego Klienta.
8. Do prawidłowego wykrywania zagrożeń przez agenta nie może być wymagane połączenie z chmurą. Skonfigurowani agenci na urządzeniach odłączonych od Internetu muszą wykrywać zagrożenia równie skutecznie, jak na urządzeniach podłączonych do Internetu.
9. Sposób wykrywania zagrożeń przez agenta musi opierać się na modelach matematycznych opracowanych z użyciem uczenia maszynowego i sztucznej inteligencji. Nie dopuszcza się rozwiązań opartych o sygnatury, huerystykę, sandboxing.
10. Aktualizacja zainstalowanych wersji agentów musi być kontrolowana przez administratora za pomocą konsoli i umożliwiać z jej poziomu inicjowanie aktualizacji agentów dla wskazanych grup urządzeń.
11. W konsoli musi być możliwość tworzenia kont administratorów oraz definiowania i przypisywania ról administracyjnych, z określonymi uprawnieniami dostępu do poszczególnych funkcji konsoli, w tym z możliwością definiowania dostępu w trybie tylko do odczytu (read-only).
12. Rozwiązanie musi być wyposażone w moduł raportowania, z możliwością wyeksportowania raportów do pliku .PNG.
13. Rozwiązanie musi legitymować się oceną AAA w testach prowadzonych przez SE Labs.

**Wymagania szczegółowe – polityki bezpieczeństwa:**

1. Możliwość grupowania urządzeń ręcznie oraz automatycznie (dynamicznie) na podstawie ich atrybutów, co najmniej: nazwa urządzenia, system operacyjny, zakres adresów IP, domena.
2. Rozwiązanie musi umożliwiać definiowanie polityk bezpieczeństwa dla urządzeń, przypisywanie zdefiniowanej polityki bezpieczeństwa do wybranego urządzenia, przypisywanie zdefiniowanej polityki bezpieczeństwa do grupy urządzeń.
3. Polityka bezpieczeństwa dla urządzeń musi określać sposób działania agenta w zakresie oferowanej przez niego funkcjonalności ochrony przed złośliwym oprogramowaniem oraz wykrywania ataków i reagowania na nie (np. włączenie lub wyłączenie konkretnych funkcjonalności).

**Wymagania szczegółowe – ochrona przed złośliwym oprogramowaniem (funkcjonalność antymalware):**

1. Agent instalowany na urządzeniach końcowych musi obsługiwać następujące platformy systemowe:

* Windows 11, 10,
* Windows Server od wersji 2012,
* MacOS od wersji 10,
* Oracle Linux Server od wersji 7,
* Debian 10,
* Ubuntu od wersji 16.04,
* Android od wersji 10,
* iOS/iPadOS od wersji 15

1. Agent musi realizować politykę bezpieczeństwa przypisaną do urządzenia.
2. Rozwiązanie musi umożliwić pełne skanowanie dysków pod kątem złośliwych plików, na żądanie lub tylko raz po instalacji z opcją automatycznego skanowania nowych i zmodyfikowanych plików.
3. Mechanizm skanowania plików musi działać w tle z niskim priorytetem.
4. Ochrona musi być realizowana predyktywnie (zapobieganie uruchomieniu kodu), a nie reaktywnie (reakcja na wykonanie kodu na urządzeniu).
5. Agent musi zapobiegać uruchomieniu złośliwego kodu z pliku w sposób automatyczny, bez udziału człowieka, podejmując decyzję w czasie poniżej 0,1 sekundy.
6. Rozwiązanie musi wykrywać zagrożenia typu ‘zero-day’.
7. Musi być dostępny mechanizm automatycznego poddawania kwarantannie plików zakwalifikowanych przez agenta, jako złośliwe.
8. Rozwiązanie powinno posiadać globalną listę plików niebezpiecznych, które zawsze mają być poddawane kwarantannie na każdym urządzeniu. Powinna być możliwość dodania na tą listę zarówno pliku zakwalifikowanego przez agenta, jak i ręcznego wpisania dowolnego pliku poprzez podanie jego skrótu SHA256.
9. Rozwiązanie powinno posiadać globalną listę plików bezpiecznych, które nie mogą być poddawane kwarantannie na żadnym urządzeniu. Powinna być możliwość dodania na tą listę zarówno pliku zakwalifikowanego przez agenta, jak i ręcznego wpisania dowolnego pliku poprzez podanie jego skrótu SHA256.
10. Rozwiązanie powinno prezentować listę plików zakwalifikowanych jako złośliwe, które nie zostały przypisane przez administratora do globalnych list. Z poziomu tej listy powinna być możliwość przypisania wybranych plików do globalnej listy plików niebezpiecznych lub globalnej listy plików bezpiecznych.
11. Rozwiązanie musi posiadać opcję automatycznego usuwania plików poddanych kwarantannie po upływie określonej liczby dni.
12. Rozwiązanie musi zapewniać ochronę pamięci, wykrywając i blokując próby uruchomienia exploitów.
13. Rozwiązanie powinno posiadać mechanizm kontroli skryptów PowerShell, Active Script, makr MS Office, Python, .NET DLR.
14. Rozwiązanie powinno posiadać mechanizm kontroli urządzeń podłączanych do portu USB. Mechanizm musi umożliwiać rozróżnienie i blokowanie urządzeń co najmniej typu: urządzenia z system Android, urządzenia z systemem iOS, urządzenia USB CD DVD RW, VMWare USB Passthrough, Windows Portable Device. Musi być możliwość stworzenia wyjątków dla wskazanych urządzeń identyfikowanych przez producenta, model, numer seryjny.
15. Rozwiązanie powinno prezentować analizę złośliwego pliku po podaniu w konsoli jego skrótu – SHA256 hash.
16. Rozwiązanie powinno mieć opcję automatycznego wysyłania kodu (pliku) do dalszej analizy przez producenta celem zaraportowanie w szczegółach zachowania złośliwego kodu.
17. Wszystkie funkcje ochronne muszą działać bez konieczności komunikacji agenta z konsolą zarządzającą, jak również w sytuacji braku połączenia urządzenia z internetem.
18. Agent musi pozwalać na współistnienie innego rozwiązania antywirusowego na urządzeniu.
19. Rozwiązanie musi umożliwiać zablokowanie możliwości instalowania, rekonfigurowania i uruchamiania nowych aplikacji na chronionym urządzeniu.

**Wymagania szczegółowe – wykrywanie ataku i reagowanie (funkcjonalność EDR):**

1. Agent instalowany na urządzeniach końcowych musi obsługiwać następujące platformy systemowe:

* Windows 11, 10,
* Windows Server od wersji 2012,
* MacOS od wersji 10.

1. Agent EDR musi w swoim działaniu wykorzystywać mechanizmy sztucznej inteligencji.
2. Rozwiązanie musi zawierać gotowe reguły wykrywania incydentów, dostarczone przez producenta, pozwalające wykrywać podejrzane działania na urządzeniu, wskazujące na zainicjowanie ataku.
3. Administrator musi mieć możliwość tworzenia własnych reguł wykrywania incydentów.
4. Musi być możliwość tworzenia zestawów reguł wykrywania, w których tylko wskazane, dowolnie wybrane reguły będą aktywne.
5. Musi być możliwość przypisania priorytetu (poziomu ważności) do reguły, co najmniej: wysoki, średni, niski, informacyjny.
6. Musi być możliwość przypisania zdefiniowanego zestawu reguł do wybranych urządzeń.
7. Musi być możliwość tworzenia wyjątków dla reguł wykrywania, tj. definiowania warunków, przy spełnieniu których aktywna reguła nie będzie traktować incydentu, jako potencjalnego ataku.
8. Musi być możliwość wysyłania powiadomienia do administratora, gdy reguła wykryje incydent.
9. Agent musi obserwować i rejestrować zdarzenia dotyczące procesów, plików, połączeń sieciowych i rejestrów na urządzeniu końcowym, aby zapewnić odpowiedni kontekst analizy w wypadku wykrycia incydentu.
10. Administrator musi mieć możliwość włączenia mechanizmu zbierania dodatkowych danych z systemu, na którym jest zainstalowany agent, w tym co najmniej: zapytań i odpowiedzi DNS, lokalnych połączeń IP, dziennika zdarzeń systemu Windows, dodatkowych atrybutów i parametrów dla poleceń wykonywanych za pomocą Powershell, dodatkowych atrybutów i parametrów dla Windows Management Instrumentation (WMI), dodatkowych informacji powiązanych z Portable Executable (PE), dodatkowych informacji uzyskiwanych z Win32 API i kernela.
11. Rozwiązanie musi umożliwiać automatyczne przesyłanie do konsoli administracyjnej szczegółowych danych dotyczących incydentów, co najmniej dla zablokowanych zagrożeń i mechanizmów ochrony pamięci.
12. Musi być możliwość zdefiniowania akcji, która zostanie automatycznie wykonana na urządzeniu w odpowiedzi na wykrycie incydentu przez regułę. Wymaga się, aby producent dostarczył w rozwiązaniu gotowe definicje takich akcji, umożliwiające co najmniej: wylogowanie wszystkich użytkowników z urządzenia, wylogowanie zdalnych użytkowników z urządzenia, zawieszenie podejrzanego procesu i jego pochodnych, zakończenie podejrzanego procesu i jego pochodnych, usunięcie wpisów z rejestru Windows, usunięcie podejrzanych plików, wyświetlenie powiadomienia, utworzenie zrzutu danych zebranych podczas wystąpienia zdarzenia.
13. Musi być możliwość definiowania własnych akcji, które zostaną wykonane na urządzeniu po wykryciu incydentu przez regułę.
14. Musi być możliwość automatycznego zbierania dodatkowych informacji o stanie urządzenia, bezpośrednio po wykryciu incydentu przez regułę. Wymaga się, aby producent dostarczył w rozwiązaniu mechanizm automatycznego zbierania dodatkowych informacji dla systemu Windows, co najmniej: zrzut ustawień rejestrów, zawartość tablicy MFT, listę aplikacji uruchomionych na urządzeniu, zawartość Event Log, historię przeglądarki internetowej.
15. Wykryte incydenty muszą być prezentowane w konsoli, jako graficzne wykresy na osi czasu. Wymagane jest prezentowanie incydentów z ostatnich 24 godzin, 7 dni i 30 dni.
16. Administrator musi mieć możliwość filtrowania prezentowanych incydentów wg priorytetu (przypisanego do reguły wykrywającej incydent).
17. Administrator musi mieć możliwość wglądu w szczegóły danego incydentu, bezpośrednio z wykresu czasowego. Szczegóły incydentu muszą pokazywać chronologię i wzajemną zależność zarejestrowanych zdarzeń, które zostały uznane za incydent.
18. Z poziomu szczegółów incydentu, administrator musi mieć możliwość zdefiniowania wyjątku dla reguły wykrywającej ten incydent, w oparciu o informacje widoczne w szczegółach zdarzeń.
19. Z poziomu szczegółów incydentu musi być możliwość wyeksportowania szczegółów incydentu do formatu .JSON, usunięcia incydentu z listy oraz zablokowania urządzenia, na którym incydent miał miejsce.
20. Administrator musi mieć możliwość wysyłania z konsoli zapytań do urządzeń w celu poszukiwania artefaktów incydentu, wg co najmniej: nazwy pliku, skrótu pliku (hash), nazwy procesu, klucza i wartości rejestru, nawiązanego połączenia sieciowego. Powinna być możliwość wysłania zapytania od razu do wszystkich urządzeń w grupie.
21. Wyniki zapytania muszą być dostępne w konsoli administracyjnej. Jeśli wynik jest pozytywny (artefakt został znaleziony), musi być możliwość wglądu w jego szczegóły oraz pobrania artefaktu z urządzenia (w przypadku pliku).
22. Administrator w momencie przeglądania wyników wyszukiwania musi mieć możliwość wykonania analizy danego obiektu pod kątem jego zachowania – wynik takiej analizy musi być dostępny w postaci graficznej.
23. Graficzny wynik analizy danego obiektu lub incydentu musi przedstawiać ścieżkę aktywności obiektu w systemie.
24. Informacje dotyczące analizy incydentu muszą zawierać informacje o tworzeniu plików, uruchamianiu procesów, operacjach zmian i tworzenia nowych wpisów.
25. Administrator musi mieć możliwość wglądu w incydent w postaci wykresu lub w postaci listy operacji jakie miały miejsce podczas incydentu.
26. Z poziomu konsoli musi być możliwość zdalnego zablokowania urządzenia, na którym incydent miał miejsce.
27. Musi istnieć możliwość exportu informacji dotyczących incydentu do pliku .CSV.
28. Agent musi gromadzić logi ze swojego działania na lokalnym dysku chronionego urządzenia. Administrator musi mieć możliwość określenia maksymalnej ilości miejsca, jakie mogą zająć logi na dysku. W przypadku wyczerpania miejsca, agent musi nadpisywać najstarsze logi.
29. Administrator musi mieć możliwość uruchomienia z poziomu konsoli, zdalnego wiersza poleceń do urządzenia.
30. Rozwiązanie musi umożliwiać z poziomu konsoli całkowite odizolowanie wskazanego urządzenia od sieci na z góry określony czas oraz ręczne odblokowanie izolacji przez podanie unikatowego kodu bezpośrednio na urządzeniu.
31. Rozwiązanie musi umożliwiać z poziomu konsoli zablokowanie komunikacji sieciowej urządzenia, z pozostawieniem jedynie komunikacji agenta z konsolą zarządzającą.

**Usługi:**

Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania, w wymienionym poniżej zakresie:

* konfiguracja konsoli administracyjnej,
* zdefiniowanie przykładowej polityki bezpieczeństwa,
* zainstalowanie agenta na 3 urządzeniach,
* szkolenie dla administratora rozwiązania,
* wsparcie w języku polskim w trybie 8x5 w dni robocze.

# 6.

# Oprogramowanie antywirusowe 100 licencji z subskrypcją do dnia 30.06.2026

**Ochrona stacji roboczych – 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.

**Ochrona antywirusowa i antyspyware:**

1. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
3. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
4. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.
5. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
6. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
7. 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.
8. 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).
9. Rozwiązanie musi posiadać opcję skanowania „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
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. Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
15. Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
16. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
17. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
18. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
19. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
20. 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.
21. Rozwiązanie musi posiadać wbudowany konektor dla programu Microsoft Outlook.
22. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu Microsoft Outlook.
23. 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).
24. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
25. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
26. Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
27. 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.
28. Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
29. Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
30. Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
31. Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
32. Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
33. Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego.
34. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
35. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
36. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
37. 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.
38. 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.
39. 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.
40. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
41. Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
42. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
43. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
44. 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.
45. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo.
46. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
47. 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.
48. 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.
49. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
50. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
51. 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.
52. 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.
53. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
54. 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.
55. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
56. W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
57. Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
58. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).
59. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
60. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
61. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
62. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
63. 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,
64. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
65. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
66. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
67. Rozwiązanie musi posiadać zaawansowany skaner pamięci.
68. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
69. 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.
70. 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.
71. 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.
72. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
73. 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.
74. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji.
75. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
76. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
77. Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
78. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
79. Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
80. W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania.
81. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
82. Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
83. Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
84. 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.
85. Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie.
86. 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.
87. W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
88. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej.
89. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
90. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
91. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
92. Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
93. 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.
94. Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
95. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
96. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
97. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
98. Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
99. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
100. Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”
101. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
102. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
103. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
104. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
105. Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet.
106. Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego do stania się do stacji roboczej za pomocą protokołu RDP i SMB.
107. Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
108. 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:
2. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
3. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
4. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
5. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
6. Rozwiązanie musi oceniać reguły zapory systemu Windows.
7. Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych.
8. Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
9. 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.
10. Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
11. Rozwiązanie musi posiadać możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
12. 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.
13. Rozwiązanie musi wykrywać modyfikację w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
14. Rozwiązanie musi posiadać możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
15. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
16. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
17. 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.
18. 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.
19. 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.
20. Rozwiązanie musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów:
21. z aplikacją lokalną, którą administrator wskazuje z listy,
22. 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 stacji roboczych – 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 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:
39. automatyczny z wyjątkami - umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł,
40. interaktywny – dla każdej nieznanej komunikacji generowane jest pytanie dla użytkownika o jej odblokowanie.
41. Rozwiązanie musi mieć możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
42. Rozwiązanie musi mieć możliwość odnotowania faktu nawiązania danego połączenia w dzienniku zdarzeń.
43. Rozwiązanie musi mieć możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.
44. Rozwiązanie musi mieć możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla profilu: Publiczny, Praca, Dom.
45. Rozwiązanie musi oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
46. Rozwiązanie musi mieć możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
47. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
48. 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 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:
2. połączenie Wi-Fi,
3. GPS,
4. usługi lokalizacyjne,
5. pamięć,
6. roaming danych,
7. roaming połączeń,
8. nieznane źródła,
9. tryb debugowania,
10. komunikacja NFC,
11. szyfrowanie pamięci masowej,
12. 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:
4. nazwę aplikacji,
5. nazwę pakietu,
6. kategorię sklepu Google Play,
7. uprawnienia aplikacji,
8. pochodzenie aplikacji z nieznanego źródła.

**Zabezpieczenia urządzenia:**

1. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej:
2. minimalny poziom zabezpieczeń i złożoność blokady ekranu,
3. maksymalną dopuszczaną liczbę błędnych prób odblokowania,
4. odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie,
5. czas, po którym automatycznie nastąpi blokada ekranu,
6. 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.

**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:
19. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
20. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
21. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
22. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
23. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
24. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
25. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
26. Rozwiązanie musi posiadać zaawansowany skaner pamięci.
27. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
28. Rozwiązanie musi oferować możliwość skanowania dysków sieciowych typu NAS.
29. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze.
30. 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.
31. 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.
32. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
33. 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.
34. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
35. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
36. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
37. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
38. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
39. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
40. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
41. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
42. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
43. Rozwiązanie ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
44. 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.
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 wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
48. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
49. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
50. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
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 programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma 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 jakiejś aktualizacji – poinformować o tym użytkownika i wyświetlić listę 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 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.
60. 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.
61. 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.
62. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
63. 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.
64. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
65. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
66. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
67. Rozwiązanie musi być wyposażone w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
68. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
69. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
70. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
71. Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania.
72. Rozwiązanie musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”.
73. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
74. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.
75. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
76. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
77. Rozwiązanie musi posiadać ochronę przed przyłączeniem komputera do sieci botnet.
78. Rozwiązanie musi mieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
79. 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.
80. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
81. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
82. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
83. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.

**Interfejs graficzny:**

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.

**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.

**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:
13. ilość znaków,
14. czy hasło ma zawierać wielkie litery,
15. czy hasło ma zawierać małe litery,
16. czy hasło ma zawierać cyfry,
17. czy hasło ma zawierać znaki specjalne,
18. okres ważności,
19. ilość nieudanych logowań,
20. możliwość zmiany hasła.
21. Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom.
22. Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku.

**Extended detection & response:**

**Serwer:**

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.
29. Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.

**Konektor:**

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. Wsparcie dla 32 i 64-bitowej wersji systemu Windows.
4. Konektor musi współpracować z produktem antywirusowym tego samego producenta.
5. Konektor nie może działać bez produktu antywirusowego tego samego producenta.
6. W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonane przez konektor.
7. Połączenie konektora do serwera zarządzającego musi być szyfrowane.
8. 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:
13. czysty,
14. podejrzany,
15. bardzo podejrzany,
16. szkodliwy.
17. 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.
18. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
19. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

**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. 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 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 dostępne w języku polskim.
6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
7. użytkowników, otrzymujących najwięcej spamu,
8. użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
9. użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
10. kont użytkowników, które mogę być podejrzane.
11. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.
12. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
13. jaka ilość wiadomości została przeskanowania,
14. wynik skanowania poszczególnej wiadomości,
15. czynność podjęta przez rozwiązanie.
16. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o:
17. zagrożeniach, które zostały wykryte,
18. na jakim koncie zostały wykryte,
19. jakie zagrożenie zostało wykryte,
20. podjętą czynność.
21. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
22. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
23. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
24. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:
25. wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
26. wprowadzenia białych i czarnych list adresów ochrony Exchange’a Online,
27. dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
28. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
29. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
30. 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.
31. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
32. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

**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 baziedanych 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 re instalacji 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), 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.

**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 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 uwierzytelnia-nie 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,
* klasyczne uwierzytelnianie (przy użyciu nazwy użytkownika i hasła).

1. 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 punkcie 28 niniejszej specyfikacji.
2. Dwuskładnikowe uwierzytelnianie nie może wymagać od użytkownika instalacji aplikacji mobilnej w telefonie - wówczas jednorazowe hasła muszą być przesyłane do użytkownika w postaci wiadomości SMS.
3. Dodatek w module ADUC musi wyświetlać informację co najmniej o dniu i godzinie ostatniej próby logowania oraz ostatniej nieudanej próby logowania użytkownika.
4. 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.
5. Administrator musi mieć możliwość odblokowania konta użytkownika w celu umożliwienia ponownego dostępu.
6. 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).
7. Administrator musi mieć możliwość podglądu informacji na temat:

* aktualnego stanu licencji,
* ilości wykorzystanych licencji (użytkowników),
* ilości pozostałych do wykorzystania wiadomości SMS.

1. Oprogramowanie przy użyciu serwera RADUIS musi umożliwiać dostęp do zabezpieczonych zasobów za pomocą klasycznej metody uwierzytelnienia (nazwa użytkownika i hasła).
2. Administrator musi mieć możliwość wyboru, którzy użytkownicy będą korzystać z dwuskładnikowego uwierzytelniania.
3. Administrator musi mieć możliwość ograniczenia dostępu przy uwierzytelnianiu metodą RADIUS do grupy użytkowników wskazanych w konfiguracji.
4. Jednorazowe hasło (OTP) generowane przez użytkowników powinno być unikalne i może być użyte tylko raz – nie dopuszcza się wielokrotnego użycia tego samego OTP.
5. Do wysyłania wiadomości SMS nie może być wymagane posiadanie własnej bramy SMS i centrali GSM.
6. Wysyłanie wiadomości SMS z hasłami jednorazowymi musi odbywać się z infrastruktury producenta rozwiązania.
7. Wysyłanie wiadomości musi być możliwe w przypadku telefonów pracujących w roamingu.

**API i SDK**

1. Producent musi udostępnić API pozwalające programistom na zintegrowanie rozwiązania z serwisem web lub oprogramowaniem wykorzystującym uwierzytelnianie w oparciu o usługę Active Directory.
2. 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).
3. 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.

**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:
6. nazwę aplikacji lub systemu operacyjnego,
7. punktacje CVSS,
8. opis wykrytej podatności,
9. wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta.
10. Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach.
11. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.
12. 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.
13. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających 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.
14. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
15. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
16. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.
17. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.
18. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.

**Usługi:**

Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, przeprowadzoną przez wykwalikowanego inżyniera.

# 7.

# Centralnie zarządzane switche – 9 szt.:

**Przełącznik sieciowy**

W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

**Parametry fizyczne platformy:**

* wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U,
* zasilanie AC 230V,
* maksymalny pobór mocy: 60 W,
* minimalny zakres temperatury pracy: 0-40ᵒC.

**Interfejsy sieciowe - wymagania minimalne:**

Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: 48 portów GE RJ-45 oraz 4 porty 10 GE SFP+.

**Zarządzanie:**

* zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS),
* wsparcie dla SNMP w wersjach 1-3,
* funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami,
* funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI,
* konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline,
* funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP),
* funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+,
* funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji,
* automatycznie wykonywane rewizje konfiguracji.

**Parametry wydajnościowe:**

* przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps,
* tablica adresów MAC o pojemności co najmniej 32k wpisów,
* opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

**Wymagane funkcje:**

* funkcja automatycznej negocjacji prędkości i duplexu dla połączeń,
* obsługa Jumbo Frames,
* obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree),
* agregacja portów zgodna ze standardem 802.3ad,
* obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q,
* obsługa routingu statycznego,
* port-mirroring,
* uwierzytelnianie 802.1x na poziomie portu,
* uwierzytelnianie 802.1x w oparciu o adres MAC,
* w ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN),
* w ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia,
* w ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN,
* obsługa protokołu sFlow.

**Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC:**

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

* centralne zarządzanie konfiguracją urządzenia,
* aktualizacja oprogramowania realizowana z systemu centralnego zarządzania,
* centralne zarządzanie sieciami VLAN,
* blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u,
* rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.,
* przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej,
* integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego,
* automatyczna detekcja i rekomendacje konfiguracji,
* przesyłanie logów na zewnętrzny serwer syslog,
* funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników,
* obsługa białych i czarnych list adresów MAC,
* wykrywanie aplikacji komunikujących się w sieci,

1. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
2. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

**Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa:**

* System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
* System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

**Gwarancja oraz wsparcie:**

System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7 minimum do dnia 30.06.2026 roku.

**Rozszerzone wsparcie serwisowe :**

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesięcy.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.

**Oferent winien przedłożyć dokumenty**:

* oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu   
  i numer infolinii telefonicznej),
* certyfikat ISO 9001 podmiotu serwisującego.

**Wdrożenie i konfiguracja:**

Od Wykonawcy wymaga się wdrożenia dostarczonego rozwiązania wraz z pełną konfiguracją i integracją   
z infrastrukturą informatyczną Zamawiającego.

Wdrożenie musi być przeprowadzone przez certyfikowanego inżyniera, posiadającego minimum 4 aktywne certyfikaty producenta oferowanego w postępowaniu rozwiązania:

• certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci (NS),

• certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej (PCS),

• certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa (SO),

• certyfikowany Specjalista w zakresie Dostępu na Krawędzi Sieci (SASE).

**Certyfikaty osobowe załączyć do oferty.**

**Opisy do wymagań ogólnych:**

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien **przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora** producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

# 8.

# Centralnie zarządzane access pointy – 5 szt.:

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
   1. temperatura 0–50°C,
   2. wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington.
3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
   1. 2.4 GHz 802.11b/g/n,
   2. 5 GHz 802.11a/n/ac/ax,
   3. 2.4/5/6 GHz 802.11a/b/g/n/ac/ax
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.
5. Urządzenie musi być wyposażone w moduł BLE.
6. Urządzenie musi być wyposażone w dwa interfejsy Ethernet 100/1000/2500/5000 Base-TX
7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3bt lub zewnętrzny zasilacz.
8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
   1. tunnel,
   2. bridge,
   3. mesh.
9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).
11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    1. MIMO – 4x4,
    2. wymagana maksymalna przepustowość dla poszczególnych modułów radiowych:
       * 1147 Mbps,
       * 2402 Mbps,
       * 4803 Mbps.
    3. Wymagana moc nadawania:
       * min. 26 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm,
       * min. 26 dBm dla pasma 5GHz z możliwością zmiany co 1dBm,
       * min. 24 dBm dla pasma 6GHz z możliwością zmiany co 1dBm.
    4. Wsparcie dla 802.11n 20/40Mhz HT,
    5. Wsparcie dla kanałów 80 i 160 MHz,
    6. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 6dBi dla pasma 5GHz, 5.5dBi dla pasma 6GHz,
    7. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy.
12. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512
13. Funkcje dodatkowe:
    1. OFDMA UL i DL,
    2. Spatial Reuse (BSS Coloring),
    3. UL-MU-MIMO,
    4. DL-MU-MIMO,
    5. Enhanced Target Wake Time (TWT),
    6. wbudowany analizator widma,
    7. wbudowane mechanizmy WIPS/WIDS.

**Gwarancja oraz wsparcie:**

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7 minimum do dnia 30.06.2026 roku.

**Rozszerzone wsparcie serwisowe:**

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesięcy.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7**.**

**Oferent winien przedłożyć dokumenty**:

* Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
* Certyfikat ISO 9001 podmiotu serwisującego.

**Wdrożenie i konfiguracja:**

Od Wykonawcy wymaga się wdrożenia dostarczonego rozwiązania wraz z pełną konfiguracją i integracją z infrastrukturą informatyczną Zamawiającego.

Wdrożenie musi być przeprowadzone przez certyfikowanego inżyniera, posiadającego minimum 4 aktywne certyfikaty producenta oferowanego w postępowaniu rozwiązania:

* certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci (NS),
* certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej (PCS),
* certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa (SO),
* certyfikowany Specjalista w zakresie Dostępu na Krawędzi Sieci (SASE).

**Certyfikaty osobowe załączyć do oferty.**

**Opisy do wymagań ogólnych:**

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): **Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora** producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

# 9.

# System do backupu danych – 1 szt.:

**Zarządzanie i magazyny:**

1. Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2024r.
2. System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.
3. Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe:
   1. obudowa rack rozmiar: 1U,
   2. pamięć RAM: 16GB,
   3. przestrzeń dostępna na przechowywanie danych: 24TB,
   4. osobne dyski SSD M.2 nVME działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego,
   5. redundantne zasilanie,
   6. interfejsy sieciowe : 2 szt. 1 Gb oraz 2 szt 10Gb,
   7. gwaracja NBD on-premise o czasie trwania analogicznym do trwania wsparcia technicznego.
4. Produkt dostępny w polskiej wersji językowej.
5. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
6. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków
7. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów
8. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych
9. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
10. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
11. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe
12. System zarządzania nie może być oparty o relacyjne bazy danych.
13. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
14. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
15. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
16. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.
17. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
18. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
19. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.
20. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
21. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
22. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
23. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych
24. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
25. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
26. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
27. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
28. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
29. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,
30. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
31. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.
32. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
33. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
34. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
35. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych.
36. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
37. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
38. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
39. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
40. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
41. System musi pozwalać na automatyczne aktualizacje oprogramowania.
42. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
43. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.
44. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
45. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
46. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
47. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
48. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
49. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
50. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
51. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
52. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
53. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
54. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental.
55. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
56. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3 oraz dedykowana chmura producenta appliance’u.
57. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, S3, nfs, iscsi, katalog lokalny
58. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).
59. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyeksponowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.
60. Możliwość generowania raportów dobowych w oparciu o harmonogram
61. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter musi być zlokalizowane na terenie Polski)
62. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)
63. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.
64. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu).

**Środowiska fizyczne i bazy danych:**

1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.
2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.
3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.
4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.
5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.
6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych.
7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.
8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.
9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.
11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.
12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).
13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.
14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

**Środowiska wirtualne:**

1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.
2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.
3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.
4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.
5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.
6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.
8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.

**Aplikacje SaaS:**

1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.
2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .PST oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji).
3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.
4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi
5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.
6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.
7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.
8. System musi umożliwiać zabezpieczenie środowisk Jira.
9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.

**Licencjonowanie i wsparcie techniczne:**

1. Wszystkie linie supportu muszą być obsługiwane w języku polskim.
2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta przez minimum   
   12 miesięcy.
3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.
4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów).
5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.
6. W ramach wsparcia technicznego Zamawiający musi mieć dostęp do tzw. Dedicated Customer Success Managera, tj. osoby po stronie Dostawcy dedykowanej do obsługi zgłoszeń technicznych, doraźnej pomocy i bieżącej pomocy w utrzymania infrastruktury Zamawiającego.
7. W ramach dokumentacji posprzedażowej Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do Dedicated Customer Success Managera.
8. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych.
9. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu.
10. Licencja umożliwia przechowywanie danych w chmurze dostarczonej bezpośrednio przez producenta w pakiecie przestrzeni 4.8 TB na czas trwania wsparcia technicznego.

**Anty-ransomware i bezpieczeństwo:**

1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").
2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System
3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.
4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.
5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczanym urządzeniu.

# 10.

# Zasilanie awaryjne – UPS – serwery – 2 szt.:

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Moc pozorna | minimum 6000VA |
| Moc rzeczywista | minimum 6000W |
| Technologia | on-line (VFI), podwójna konwersja |
| Sprawność przy pracy sieciowej | ˃ 95 % |
| Sprawność przy pracy bateryjnej | ˃ 92 % |
| Typ obudowy | rack, max 5U (z bateriami) |
| **Wejście** |  |
| Napięcie wejściowe | 220/230/240 VAC |
| Częstotliwość napięcia wejściowego | minimum 46~54 Hz lub 56~64 Hz |
| Zakres napięcia wejściowego | minimum 110 ÷ 300 V AC ± 3% przy 50% obciążenia |
| Kształt napięcia wyjściowego | sinusoidalny |
| Czas przełączania sieć – bateria | 0ms |
| Współczynnik odkształceń prądu wejściowego THDi | do 3% przy 100% obciążenia |
| **Wyjście** |  |
| Napięcie wyjściowe | 220/230/240 VAC |
| Częstotliwość napięcia wyjściowego | minimum 50Hz/60Hz ± 0,1Hz |
| Kształt napięcia wyjściowego na pracy bateryjnej | sinusoidalny |
| Współczynnik odkształceń prądu wejściowego THD | ≦ 2 % (obciążenie liniowe) |
| Baterie wewnętrzne w UPS lub w zewnętrznym module bateryjnym | minimum 12V 9Ah; szczelne, bezobsługowe |
| Czas podtrzymania dla obciążenia 80% - przy zastosowaniu wewnętrznych baterii lub w 1 zewnętrznym module bateryjnym producenta UPS | minimum 10 minut |
| **Pozostałe** |  |
| Współpraca z 16 lub 20 bateriami | wymagane |
| Wejście zasilania | listwa zaciskowa / terminal śrubowy |
| Ilość i typ gniazd wyjściowych | listwa zaciskowa / terminal śrubowy |
| Obciążalność w trybie sieciowym AC | 100%~110%:10min; 110%~130%:1min; >130%:1s |
| Sygnalizacja | Wyświetlacz LCD |
| Informacje wyświetlane na panelu LCD | poziom obciążenia (w %),  poziom naładowania baterii (w %),  praca z sieci/baterii/ładowanie baterii,  przeciążenie, niski poziom baterii,  bateria nie podłączona lub błąd baterii,  tryb ECO/Bypass, napięcie wej/wyj,  częstotliwość wej/wyj, błąd + numer błędu, czas podtrzymania bateryjnego,  wyłączenie dźwięku. |
| Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych (producenta) | wymagane |
| Interfejs komunikacyjny | RS232, USB, SNMP |
| Możliwość zastosowania karty SNMP w innych rozwiązaniach 1-fazowych i 3-fazowych tego samego producenta | wymagane |
| Zabezpieczenia | minimum przeciwzwarciowe, przeciwprzepięciowe, przeciążeniowe |
| Złącze EPO | wymagane |
| Wsporniki do montażu w szafie rack | wymagane |
| Waga UPS | do 18 kg |
| Wymiary UPS - wersja RACK | nie większe niż: wysokość 2U; głębokość 620 mm |
| Waga Moduł Bateryjny - jeżeli występuje | do 49 kg |
| Wymiary Moduł Bateryjny - wersja RACK - jeżeli występuje | nie większe niż: wysokość 3U; głębokość 720 mm |
| Gwarancja | minimum 24 miesiące na elektronikę i 24 miesiące na akumulatory |
| Serwis | autoryzowany serwis producenta zlokalizowany w Polsce |
| naprawa w maksymalnie 5 dni roboczych |
| serwis realizowany w systemie door to door |
| gwarancja realizowana wyłącznie przez Autoryzowany Serwis Producenta |
| Oprogramowanie | oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS |
| wsparcie dla systemów: Windows, Windows Server oraz systemów wirtualizacji |
| wymagane wsparcie producenta w języku polskim (telefoniczne oraz mailowe) |
| Możliwość monitorowania i konfiguracji UPS przez przeglądarkę WWW | wymagane |
| Oświadczenia / dokumenty (**załączyć do oferty**) | deklaracja zgodności CE |
| normy: EN/IEC 62040-1, EN/IEC 62040-2  RoHS |
| oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji |
| certyfikat lub oświadczenie producenta o posiadaniu przez oferenta statusu Autoryzowanego Partnera - mającego wiedzę w zakresie doboru i sprzedaży zasilaczy UPS |

# 11.

# Zasilanie awaryjne – UPS – stacje robocze – 68 szt.:

|  |  |
| --- | --- |
| **Parametr** | **Wymagania minimalne** |
| Moc pozorna | minimum 650VA |
| Moc rzeczywista | minimum 360W |
| Technologia | minimum line-interactive |
| Typ obudowy | tower |
| **Wejście** |  |
| Napięcie wejściowe | 220/230/240 VAC |
| Zakres napięcia wejściowego | 165-290 VAC |
| Częstotliwość | minimum 50/60Hz – automatyczne wykrywanie |
| **Wyjście** |  |
| Regulacja napięcia | minimum +/- 10 % |
| Kształt napięcia wyjściowego | minimum symulowana sinusoida |
| Typowy czas przełączania | 2-6 ms |
| **Baterie** |  |
| Baterie wewnętrzne w UPS | minimum 12V 7Ah; szczelne, bezobsługowe |
| Czas podtrzymania (50 % Pmax) | minimum 5 minut |
| **Pozostałe** |  |
| Wejście zasilania | kabel zamontowany na stałe w obudowie UPS zakończony wtykiem PL/FR |
| Ilość i typ gniazd wyjściowych | minimum 2 gniazda Schuko z podtrzymaniem |
| Stabilizacja napięcia AVR Boost & Buck | wymagana |
| Filtr RJ45 | wymagany |
| Funkcja autorestartu po powrocie zasilania | wymagana |
| Funkcja zimnego startu | wymagana |
| Sygnalizacja | Wyświetlacz LCD, dźwiękowa |
| Informacje wyświetlane na panelu LCD | minimum napięcie wejściowe i wyjściowe, poziom obciążenia, poziom naładowania baterii, praca z sieci/baterii, przeciążenie, niski poziom baterii |
| Interfejs komunikacyjny | USB |
| Zabezpieczenia | minimum przed zwarciem, przeciążeniem, rozładowaniem |
| Alarmy dźwiękowe | minimum informujące o trybie bateryjnym, rozładowaniu baterii, przeciążeniu, awarii |
| Waga UPS | do 4,5 kg |
| Wymiary UPS | nie większe niż: głębokość 290mm, szerokość 105mm, wysokość 145mm |
| Gwarancja | minimum 24 miesiące na elektronikę i 12 miesięcy na baterie |
| Serwis | autoryzowany serwis producenta zlokalizowany w Polsce. |
| naprawa w maksymalnie 14 dni roboczych |
| serwis realizowany w systemie door to door |
| Oprogramowanie | oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS |
| wsparcie dla systemów: Windows, Linux |
| wymagane wsparcie producenta w języku polskim (telefoniczne oraz mailowe) |
| Certyfikaty producenta (załączyć do oferty) | deklaracja zgodności CE |
| Oświadczenia / dokumenty  (**załączyć do oferty**) | oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji |
| certyfikat lub oświadczenie producenta o posiadaniu przez oferenta statusu Autoryzowanego Partnera - mającego wiedzę w zakresie doboru i sprzedaży zasilaczy UPS |

# 12.

# Agregat prądotwórczy – 1 szt.:

|  |  |
| --- | --- |
| **Parametr** | **Wymagania** |
| Silnik | silnik diesel, preferowani producenci silnika (Yanmar, Perkins, Iveco) |
| Paliwo | olej napędowy |
| Moc znamionowa | minimum 50kVA / 40kW |
| Moc maksymalna | minimum 55kVA / 44kW |
| Napięcie wyjściowe | 400 / 230 V AC |
| Prąd maksymalny | 79A |
| Stabilizacja napięcia | minimum +/- 1% |
| Regulator obrotów silnika | mechaniczny |
| Układ chłodzenia | ciecz chłodząca |
| Pojemność zbiornika paliwa | minimum 100l |
| Zużycie paliwa przy 75% obciążenia (w pracy ciągłej) | maksymalnie 7,5l/h |
| Prądnica | preferowani producenci prądnicy (Stamford, Leroy Somer) |
| Konstrukcja prądnicy | samowzbudna, bezszczotkowa |
| Napięcie | 400 / 230 V AC |
| Częstotliwość | 50Hz |
| Klasa izolacji | H |
| Stopień ochrony | IP23 |
| System kontroli AVR (pełna stabilizacja napięcia) | wymagane |
| Sterownik agregatu z ekranem LCD i menu w języku polskim, zabezpieczony przed dostępem osób trzecich | wymagane |
| Obudowa | agregat w obudowie wyciszonej, odpornej na warunki atmosferyczne |
| Poziom hałasu | maksymalnie 75 dB(A) z 7 metrów |
| Gniazda | zestaw gniazd odbioru mocy: 1 x 63A, 1 x 32A, 1x 16A, 2 x 16A 230V |
| Wymiary agregatu (długość/szerokość/wysokość) | nie większe niż 2550x100x1700 mm |
| Waga agregatu | Nie większa niż 1100kg |
| **Dodatkowe wymagania** | |
| Agregat fabrycznie nowy, wyprodukowany w 2024 roku | wymagane |
| Agregat dostarczany w stanie gotowym do użytku, zalany płynami (poza paliwem) | wymagane |
| Agregat wyposażony w akumulatory rozruchowe oraz ładowarkę akumulatorów | wymagane |
| Agregat przystosowany do pracy ciągłej: minimum 24 godziny | wymagane |
| Przycisk wyłączania awaryjnego | wymagane |
| Układ SZR (samoczynne załączenie rezerwy) | wymagane |
| Wskaźnik poziomu paliwa | wymagane |
| Rurka spustowa oleju ułatwiająca wymianę oleju | wymagane |
| Gwarancja | minimum: 24 miesiące (jako zasilanie awaryjne) - przy 4 płatnych przeglądach gwarancyjnych |
| **Dokumenty – dołączyć do oferty** | |
| Instrukcja obsługi zespołu prądotwórczego | wymagane |
| Karty katalogowe agregatu wraz z danymi technicznymi | wymagane |
| Polisę lub inny dokument potwierdzający zawarcie ubezpieczenia odpowiedzialności cywilnej (zarówno kontraktowej, jak i deliktowej) Wykonawcy w związku z prowadzoną przez niego działalnością (w szczególności działalnością związaną z przedmiotem Umowy) oraz posiadanym mieniem z sumą gwarancyjną w wysokości nie mniejszej niż 1 000 000,00 zł | wymagane |

W skład agregatu prądotwórczego powinna wchodzić instalacja paliwowa, smarowania, chłodzenia i elektryczno-rozruchowa oraz panel kontrolno-sterujący i wyłącznik główny.

**Przeglądy okresowe:**

Wykonywanie okresowych przeglądów agregatu prądotwórczego w terminach i zgodnie z zakresem przewidzianym dokumentacją techniczno-ruchową oraz instrukcją eksploatacji producenta. Informację o zamiarze wykonania przeglądu należy przekazać do Zamawiającego na co najmniej 4 dni robocze przed jego planowanym terminem. Każdy przegląd należy potwierdzić protokołem przeglądu z wyszczególnionym wykazem wykonanych prac. Protokół przeglądu należy dostarczyć do Zamawiającego w terminie do 7 dni roboczych licząc od dnia wykonania przeglądu.

**Wykonawca w dniu odbioru zobowiązany jest do dostarczenia dokumentacji zawierającej w szczególności:**

1. Protokół odbioru
2. Karta gwarancyjna agregatu prądotwórczego

# 13.

# Szkolenia z zakresu cyberbezpieczeństwa dla pracowników oraz kadry kierowniczej

Wykonawca zapewni szkolenie (min. 1 dzień) stacjonarne lub zdalne, z podziałem na maksymalnie 20 osobowe grupy.

Szkolenie musi być przeprowadzone przez certyfikowanego inżyniera, posiadającego aktualne certyfikaty CISSP oraz CEH.

**Certyfikaty osobowe załączyć do oferty.**

Zakres szkolenia:

**Moduł 1: Zagrożenia dla bezpieczeństwa danych:**

* przechwycenie przez niepowołane osoby (dane w transmisji, dane "w spoczynku"),
* utrata danych i utrata dostępu do danych w wyniku ataku (włamanie, wirus, trojan, ransomware),
* utrata danych i utrata dostępu do danych w wyniku awarii (przerwa w zasilaniu, awaria urządzeń, awaria nośników,
* utrata dostępu do danych w wyniku utraty danych uwierzytelniających,
* straty wynikające z naruszenia bezpieczeństwa danych.

**Moduł 2: Zabezpieczenie danych przed przechwyceniem przez niepowołane osoby lub ich utratą w wyniku ataku:**

* szyfrowanie danych (w transmisji, w spoczynku,
* bezpieczeństwo sieci lokalnej (kontrola dostępu do sieci przewodowej, DMZ, odseparowanie WiFi),
* ograniczanie dostępu do udostępnianych danych (udostępnianie wybranych zasobów, dostęp dla określonych użytkowników),
* ochrona przed włamaniem,
* silne hasła,
* ochrona haseł i kluczy - dobre praktyki,
* uwierzytelnianie dwuskładnikowe, biometryczne, przy pomocy certyfikatu,
* korzystanie z poczty elektronicznej - dobre praktyki w zakresie ochrony przed phishingiem i malware,
* oprogramowanie antywirusowe / chroniące komputer,
* aktualizacje systemu i oprogramowania,
* nieużywanie nieautoryzowanego oprogramowania,
* nie daj się podejść oszustowi,
* fizyczne zabezpieczenia danych (dostęp do urządzeń, nośników, pomieszczeń, procedury postępowania z niewykorzystywanymi już nośnikami, zasada "czystego biurka"),
* procedury dotyczące używania urządzeń prywatnych (praca zdalna, BYOD).

**Moduł 3: Zabezpieczenie danych przed utratą:**

* prewencyjna ochrona przed utratą danych w wyniku zaniku zasilania (UPS, sprawne baterie w laptopach, redundancja zasilania). Prewencyjna ochrona przed utratą danych lub dostępu do danych w wyniku innej awarii (konserwacja sprzętu, redundancja urządzeń / klastry, umowy serwisowe),
* kopie zapasowe.

**Moduł 4: Zabezpieczenie danych przed utratą dostępu w wyniku utraty danych uwierzytelniających:**

* dostęp administracyjny (zapasowe konta administracyjne, wielość administratorów, umowy),
* przechowywanie haseł.

# 14.

# Szkolenia specjalistyczne dla administratorów w zakresie planowanych do zastosowania środków bezpieczeństwa

1. **System do zarządzania siecią**

Szkolenie musi być przeprowadzone przez certyfikowanego inżyniera, posiadającego aktywny certyfikat producenta oferowanego w postępowaniu rozwiązania do zarządzania siecią. **Certyfikat załączyć do oferty**.

Szkolenie musi zakończyć się zdobyciem certyfikatu potwierdzającego nabycie praktycznej wiedzy o efektywnym zarządzaniu siecią przy pomocy wdrożonego oprogramowania.

**Zakres szkolenia:**

1. **Wprowadzenie:**

* moduły,
* wymagania sprzętowe,
* porty komunikacyjne,

1. **Instalacja programu:**

* instalacja,
* zarządzanie licencją,
* wstępna konfiguracja systemu,
* instalacja agentów.

1. **Wykrywanie i monitorowanie urządzeń:**

* zarządzie urządzeniami i mapami,
* wykrywanie sieci,
* monitorowanie serwisów,
* monitorowanie wydajności urządzenia i systemu,
* monitorowanie serwerów poczty i WWW,
* monitorowanie routerów i switch’y,
* monitorowanie urządzeń przez SNMP / serwer pułapek SNMP,
* serwer pułapek Syslog.

1. **Inwentaryzacja sprzętu i oprogramowania:**

* oprogramowanie – zarządzanie licencjami i audyt legalności oprogramowania,
* sprzęt – audyt konfiguracji sprzętowej,
* informacje systemowe,
* zarządzanie paczkami MSI,
* zarządzanie zasobami.

1. **Monitorowanie aktywności użytkowników:**

* zarządzanie użytkownikami i grupami / Integracja z AD,
* podsumowanie czasu pracy i przerw użytkownika,
* odwiedzane strony WWW,
* użycie aplikacji,
* zrzuty ekranu,
* blokowanie aplikacji i stron WWW,
* monitorowanie poczty,
* monitorowanie wydruków.

1. **Kontrola dostępu do urządzeń:**

* prawa dostępu,
* urządzenia,
* zaufane jednostki,
* audyt.

1. **Raporty:**

* tworzenie raportów,
* raporty na żądanie,
* raporty automatyczne.

1. **Alarmowanie:**

* zarządzanie alarmami,
* zdarzenia.

1. **System do ochrony poczty**

Szkolenie musi być przeprowadzone przez certyfikowanego inżyniera, posiadającego minimum 4 aktywne certyfikaty producenta oferowanego w postępowaniu systemu do ochrony poczty na poziomie:

* certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci (NS),
* certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej (PCS),
* certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa (SO),
* certyfikowany Specjalista w zakresie Dostępu na Krawędzi Sieci (SASE).

Szkolenie musi zakończyć się zdobyciem certyfikatu potwierdzającego nabycie praktycznej wiedzy o efektywnym zarządzaniu systemem do ochrony poczty.

**Zakres Szkolenia:**

**Podstawy i Konfiguracja**

1. **Wprowadzenie do systemu ochrony poczty:**

* omówienie architektury systemu,
* zastosowania i korzyści z używania systemu,
* przegląd interfejsu użytkownika (GUI) i dostępnych opcji administracyjnych.

1. **Instalacja i wstępna konfiguracja:**

* sprzętowe wymagania instalacyjne,
* podstawowa konfiguracja przez CLI oraz GUI,
* ustawienia sieciowe (adres IP, gateway, DNS).

1. **Zasady zabezpieczeń poczty:**

* omówienie polityk bezpieczeństwa poczty,
* konfiguracja filtrów antywirusowych i antyspamowych,
* ustalanie reguł ochrony przed phishingiem i innymi atakami.

**Zarządzanie użytkownikami i politykami**

1. **Konfiguracja użytkowników i domen:**

* tworzenie i zarządzanie kontami użytkowników,
* konfiguracja i zarządzanie domenami,
* ustalanie indywidualnych reguł dla użytkowników (np. ograniczenia).

1. **Praca z politykami i filtrami:**

* tworzenie polityk dostępu,
* konfiguracja listy dozwolonych/zakazanych nadawców,
* zasady dotyczące załączników i skanowania ich zawartości.

1. **Zarządzanie przepływem poczty:**

* konfiguracja i zarządzanie przepływem poczty przychodzącej i wychodzącej,
* tematy związane z przeciwdziałaniem spamowi i kontrolą ruchu,
* szyfrowanie.

**Monitorowanie i raportowanie**

1. **Monitorowanie i utrzymywanie systemu:**

* użycie narzędzi monitorujących w systemie,
* analiza danych z logów,
* śledzenie wydajności systemu.

1. **Raportowanie:**

* generowanie i interpretacja raportów,
* ustawienia powiadomień i harmonogramów raportów.

**Diagnostyka i wsparcie techniczne**

1. **Strategie utrzymania i wsparcia:**

* zasady aktualizacji oprogramowania i sprzętu,
* planowanie kopii zapasowych i przywracania systemu,
* kontakty do wsparcia technicznego i zasoby online.

1. **Rozwiązywanie problemów**
2. **System do zbierania i analizy logów**

Szkolenie musi być przeprowadzone przez certyfikowanego inżyniera, posiadającego minimum 4 aktywne certyfikaty producenta oferowanego w postępowaniu systemu do zbierania i analizy logów na poziomie:

* certyfikowany Specjalista w zakresie Bezpieczeństwa Sieci (NS),
* certyfikowany Specjalista w zakresie Bezpieczeństwa Chmury Publicznej (PCS),
* certyfikowany Specjalista w zakresie Operacji Bezpieczeństwa (SO),
* certyfikowany Specjalista w zakresie Dostępu na Krawędzi Sieci (SASE).

Szkolenie musi zakończyć się zdobyciem certyfikatu potwierdzającego nabycie praktycznej wiedzy o efektywnym zarządzaniu systemem do zbierania i analizy logów.

**Zakres Szkolenia:**

**Podstawowa Konfiguracja Sieciowa**

1. **Skonfigurowanie Adresu IP:**

* przydzielanie statycznego adresu IP do urządzenia FAZ,
* konfiguracja adresacji IP w różnych podsieciach,
* rozwiązywanie problemów związanych z konfliktem adresów IP.

1. **Konfiguracja Maski Podsieci:**

* zrozumienie i obliczanie maski podsieci,
* implementacja odpowiednich masek podsieci dla różnych segmentów sieci,
* diagnostyka problemów z komunikacją między podsieciami.

1. **Ustawienie Bramy Domyślnej:**

* konfiguracja bramy domyślnej dla urządzeń w sieci lokalnej,
* testowanie łączności z bramą domyślną,
* konfiguracja tras statycznych i dynamicznych.

1. **Konfiguracja Serwerów DNS:**

* dodawanie i priorytetyzowanie serwerów DNS,
* sprawdzanie poprawności konfiguracji DNS poprzez narzędzia diagnostyczne,
* rozwiązywanie problemów z rozpoznawaniem nazw.

**Rejestracja Urządzeń**

1. **Dodanie Urządzeń do Analizy:**

* procedury dodawania różnych typów urządzeń (routery, switche, serwery),
* automatyczne wykrywanie i ręczne dodawanie urządzeń,
* konfiguracja parametrów urządzeń do optymalizacji logowania.

1. **Weryfikacja Poprawności Rejestracji Urządzeń:**

* metody testowania poprawności rejestracji,
* rozwiązywanie problemów z rejestracją,
* monitorowanie stanu połączenia urządzeń.

**Konfiguracja Logowania**

1. **Skonfigurowanie Urządzeń do Wysyłania Logów do Analizy:**

* wybór protokołów logowania (Syslog, SNMP, WMI),
* konfiguracja parametrów logowania dla różnych urządzeń,
* zarządzanie buforami logów i zapobieganiem utracie danych.

1. **Weryfikacja Poprawności Konfiguracji Logowania:**

* testowanie konfiguracji logowania,
* rozwiązywanie problemów z przesyłaniem logów,
* monitorowanie i raportowanie stanu logowania.

**Konfiguracja Administratorów**

1. **Utworzenie Kont Administratorów:**

* procedury tworzenia kont administracyjnych,
* konfiguracja zabezpieczeń konta (hasła, uwierzytelnianie dwuskładnikowe),
* zarządzanie sesjami i prawami dostępu administratorów.

1. **Ustawienie Odpowiednich Poziomów Uprawnień:**

* definiowanie ról i przypisywanie uprawnień,
* zarządzanie politykami dostępu i audytowanie działań administratorów,
* tworzenie i zarządzanie grupami użytkowników.

**Alerty i Powiadomienia**

1. **Konfiguracja Powiadomień E-mail:**

* konfiguracja serwerów SMTP do wysyłania powiadomień,
* personalizacja szablonów e-mailowych dla różnych zdarzeń,
* testowanie i weryfikacja dostarczalności e-maili.

1. **Ustawienie Alertów dla Różnych Zdarzeń Systemowych i Zabezpieczeń:**

* tworzenie reguł alertów na podstawie specyficznych zdarzeń,
* konfiguracja eskalacji powiadomień,
* monitorowanie i zarządzanie aktywnymi alertami.

**Polityki Logowania**

1. **Ustawienie Rodzajów Logów, które Mają Być Przechowywane:**

* definiowanie kategorii logów (np. logi ruchu, logi zdarzeń),
* konfiguracja selektywnego logowania w celu optymalizacji wydajności,
* archiwizacja i przenoszenie starych logów do zewnętrznych zasobów.

1. **Konfiguracja Polityk Logowania:**

* tworzenie i zarządzanie politykami logowania,
* implementacja reguł dla różnych typów zdarzeń,
* przegląd i aktualizacja polityk na podstawie zmieniających się potrzeb i zagrożeń.

**Retencja Danych**

1. **Ustawienie Okresów Retencji dla Różnych Typów Logów:**

* definiowanie okresów przechowywania dla logów bezpieczeństwa, operacyjnych i innych,
* automatyzacja usuwania starych logów zgodnie z politykami retencji,
* audytowanie i raportowanie przestrzegania polityk retencji.

1. **Zarządzanie Miejscem na Dysku Poprzez Polityki Retencji:**

* monitorowanie zużycia przestrzeni dyskowej,
* implementacja strategii przechowywania danych w chmurze,
* optymalizacja przestrzeni dyskowej poprzez kompresję i de-duplikację logów.

**Tworzenie Pulpitów Nawigacyjnych (Dashboards)**

1. **Konfiguracja Pulpitów Nawigacyjnych dla Monitorowania w Czasie Rzeczywistym:**

* tworzenie i personalizacja interaktywnych dashboardów,
* integracja różnych źródeł danych na pulpitach nawigacyjnych,
* implementacja widgetów i graficznych reprezentacji danych.

1. **Przykłady Zastosowań Pulpitów Nawigacyjnych:**

* monitorowanie stanu sieci i urządzeń,
* wizualizacja trendów bezpieczeństwa i wykrytych incydentów,
* analiza wydajności systemów IT.

**Konfiguracja Raportów**

1. **Tworzenie Szablonów Raportów:**

* definiowanie formatów i zawartości raportów,
* personalizacja raportów według potrzeb odbiorców,
* integracja logów z zewnętrznymi narzędziami raportującymi.

1. **Ustalanie Harmonogramów Generowania Raportów:**

* automatyzacja cyklicznego generowania raportów,
* dystrybucja raportów do odpowiednich interesariuszy,
* monitorowanie i zarządzanie harmonogramami.

**Polityki Bezpieczeństwa**

1. **Ustawienie Polityk Zabezpieczeń i Zgodności:**

* definiowanie polityk bezpieczeństwa zgodnie z najlepszymi praktykami i regulacjami prawnymi,
* implementacja polityk zgodności (np. RODO, HIPAA),
* audytowanie przestrzegania polityk i zarządzanie wyjątkami.

1. **Konfiguracja Reguł Dostępu i Polityk Zgodności z Przepisami:**

* tworzenie i egzekwowanie reguł dostępu do danych i zasobów,
* regularne przeglądy i aktualizacje polityk zgodności,
* implementacja mechanizmów śledzenia i audytu.

**Testowanie Konfiguracji**

1. **Sprawdzenie Poprawności Konfiguracji Poprzez Testy Funkcjonalne:**

* przeprowadzanie testów w celu weryfikacji poprawności konfiguracji,
* analiza wyników testów i identyfikacja problemów,
* dokumentacja i wprowadzenie poprawek na podstawie testów.

1. **Symulacje Zdarzeń i Ich Analiza:**

* tworzenie scenariuszy testowych dla różnych zdarzeń bezpieczeństwa,
* analiza zachowań systemu podczas symulacji,
* ocena skuteczności konfiguracji zabezpieczeń.

**Weryfikacja Integracji**

1. **Potwierdzenie, że Wszystkie Urządzenia Są Poprawnie Zintegrowane:**

* przegląd listy zintegrowanych urządzeń i ich statusów,
* testy integracyjne dla potwierdzenia poprawności współdziałania,
* rozwiązywanie problemów z integracją i komunikacją.

1. **Weryfikacja, że Urządzenia Wysyłają Logi do Analizy:**

* monitorowanie przepływu logów z urządzeń do systemu FAZ,
* weryfikacja poprawności i kompletności danych logów,
* analiza i raportowanie stanu logowania oraz wykrytych anomalii.

1. **System antywirusowy**

Szkolenie musi być przeprowadzone przez wykwalifikowanego inżyniera, posiadającego kompetencje w zakresie instalacji i konfiguracji oferowanego w postępowaniu systemu antywirusowego.

Szkolenie musi zakończyć się zdobyciem certyfikatu potwierdzającego nabycie praktycznej wiedzy o efektywnym zarządzaniu systemem antywirusowym.

**Zakres szkolenia:**

1. **Instalacja środowiska:**

* instalacja serwera zarządzającego,
* instalacja modułu zarządzającego urządzeniami mobilnymi,
* instalacja konsoli zarządzającej,
* instalacja skanera sieciowego.

1. **Zarządzanie środowiskiem:**

* omówienie opcji dostępnych z poziomu interfejsu administratora,
* omówienie opcji dostępnych z poziomu interfejsu użytkownika,
* podstawowa konfiguracja serwera zarządzającego,
* instalacja agentów zarządzających,
* instalacja produktów zabezpieczających,
* administracja grupami statycznymi,
* administracja grupami dynamicznymi,
* konfiguracja i dystrybucja polityk.

1. **Raportowanie środowiskiem:**

* analiza dzienników zdarzeń,
* generowanie przykładowych raportów.