## **Załącznik nr 1**

 **do umowy nr ………………. z dnia …………………….**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

1. **Obecnie Urząd Miasta i Gminy Szamotuły posiada licencję WithSecure Business Suite Premium ważną do 31.03.2025 r.
Przedmiot zamówienia: Dostawa licencji oprogramowania antywirusowego, – 28 szt. licencji (w tym 3 serwery) na okres do dnia 30.06.2026 r., zgodnie z poniższymi wymaganiami:**

Ochrona antywirusowa stacji roboczych wspiera następujące systemy operacyjne:

* Microsoft Windows 10
* Microsoft Windows 11

Ochrona antywirusowa serwerów wspiera następujące systemy operacyjne:

* Microsoft Windows Server 2016 Standard
* Microsoft Windows Server 2016 Essentials
* Microsoft Windows Server 2016 Datacenter
* Microsoft Windows Server 2016 Core
* Microsoft Windows Server 2019 Standard
* Microsoft Windows Server 2019 Essentials
* Microsoft Windows Server 2019 Datacenter
* Microsoft Windows Server 2019 Core
* Microsoft Windows Server 2022

Dodatkowo wspierane serwery terminalowe:

* Microsoft Windows Terminal/RDP Services
* Citrix XenApp 5.0
* Citrix XenApp 6.0
* Citrix XenApp 6.5
* Citrix XenApp 7.5, 7.6, 7.14, 7.15

Ochrona antymalware

1. Ochrona realizowana jest na wielu poziomach tj. na poziomie plików, sieci i urządzeń zewnętrznych.
2. Rozwiązanie wyposażone jest w mechanizmy do wykrywania różnego typu malware, w tym m.in. ransomware, koni trojańskich, robaków, wirusów itp.
3. Rozwiązanie wyposażone jest w silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu spyware i riskware.
4. Aktualizacje baz definicji wirusów dostępne są 24h na dobę na serwerze producenta, możliwa jest zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
5. System posiada możliwość dystrybuowania aktualizacji baz definicji wirusów, aktualizacji oprogramowania zainstalowanego na stacji końcowej oraz polityk bezpieczeństwa za pomocą serwera pośredniczącego. Serwer pośredniczący pobiera aktualizacje oprogramowania, jak i bazy antywirusowe, z serwerów producenta, a następnie dystrybuuje je w sieci lokalnej.
6. Rozwiązanie umożliwia wywołanie skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
7. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
8. Rozwiązanie pozwala na wywołania skanowania po uruchomieniu systemu operacyjnego oraz po zalogowaniu użytkownika.
9. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
10. Rozwiązanie posiada możliwość wywołania skanowania wszystkich plików, tylko określnych rozszerzeń plików a także ich wykluczanie.
11. Rozwiązanie posiada możliwość skanowania dysków przenośnych takich jak pendrive, dyski zewnętrzne, czy dyski sieciowe.
12. Rozwiązanie pozwala na skanowanie na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
13. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
14. Rozwiązanie wykorzystuje przyrostowe (inkrementalne) pobieranie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
15. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
16. Rozwiązanie nie wymaga restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
17. Rozwiązanie wykorzystuje w swoim działaniu heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
18. Rozwiązanie pozwala na wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”, „rootkit” oraz ataki typu 0-day.
19. Rozwiązanie wykorzystuje mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), analizujący podejrzane pliki wykonywalne.
20. Rozwiązanie pozwala na skanowanie plików skompresowanych obejmujące najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
21. Skaner antymalware pozwala na integrację z AMSI
22. Ochrona plików w czasie rzeczywistym pozwala na wykluczenie ze skanowania procesów.
23. Funkcja skanowania dysków sieciowych pozwala na skanowanie wszystkich plików, do których uzyskiwany jest dostęp lub tylko plików wykonywanych z takich zasobów.
24. Użytkownik ma możliwość uwolnienia pliku poddanego kwarantannie.
25. Uwolnienie pliku z kwarantanny odbywa się po podaniu hasła ustalonego przez administratora.
26. W przypadku wykrycia szkodliwego pliku rozwiązanie umożliwia pojęcie akcji automatycznej kwarantanny pliku, automatycznego leczenia, automatycznego usunięcia pliku, automatycznej zmiany nazwy pliku, tylko zgłoszenia infekcji lub podjęcia decyzji przez użytkownika.
27. Administrator posiada możliwość określenia reakcji silnika skanującego w odniesieniu do typu wykrytego zagrożenia.
28. Osobny typ reakcji może być określny dla malware, riskware i spyware.
29. Rozwiązanie zawiera funkcje logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów możliwy jest z poziomu GUI aplikacji.
30. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
31. Administrator ma możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.

Ochrona ruchu HTTP

1. Rozwiązanie skanuje na komputerze klienckim, dane pobierane i wysyłane przy pomocy protokołu http.
2. Administrator posiada możliwość blokowania na komputerze klienckim określonego rodzaju zawartości, nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http z witryn o nieokreślonej reputacji
3. Rozwiązanie realizuję ochronę podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
4. Rozwiązanie pozwala na graficzną informację dotycząca reputacji witryn wyświetlanych w wynikach wyszukiwania za pomocą wyszukiwarek takich jak Google, Bing.
5. Rozwiązanie zabezpiecza połączenia do witryn skategoryzowanych przez producenta jako ‘bankowość elektroniczna’ poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia np. z witryną banku.
6. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z daną witryną HTTPS.
7. Rozwiązanie posiada możliwość zablokowania uruchamiania narzędzi skryptowych i commandline podczas wyświetlania witryn określonych jako bankowość internetowa.
8. Rozwiązanie posiada możliwość usuwania zawartości schowka systemowego podczas zakończenia sesji z witrynami związanymi z bankowością online.
9. Rozwiązanie posiada możliwość blokowania narzędzi dostępu zdalnego podczas korzystania z witryn określonych jako bankowość internetowa lub określonych na liście przez administratora.

Kontrola aplikacji

1. Rozwiązanie posiada wbudowany mechanizm kontroli aplikacji.
2. Administrator ma możliwość blokowania uruchomienia aplikacji na stacji końcowej.
3. Blokowanie możliwości uruchomienia aplikacji na stacji końcowej umożliwia identyfikację aplikacji, co najmniej na podstawie identyfikatora SHA1, SHA256, nazwy pliku, nazwy produktu, wydawcy, wersji pliku.
4. Mechanizm kontroli aplikacji pozwala na kontrolę co najmniej zdarzeń takich jak, uruchamianie aplikacji, uruchamianie instalacji, uruchamianie procesu, ładowania biblioteki dynamicznej, dostępu do pliku.
5. Mechanizm kontroli aplikacji pozwala na tworzenie wielu profili i stosowania ich w zależności od potrzeb.
6. Mechanizm kontroli aplikacji pozwala na ustawienie domyślnej akcji w tym zezwolenia, zablokowania, zgłoszenia dla uruchamianych aplikacji.

Zapora sieciowa

1. Rozwiązanie posiada możliwość zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
2. Mechanizm kontroli zapory ogniowej posiada wbudowane predefiniowane profile.
3. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
4. Administrator posiada możliwość określenia domyślnej reakcji dla nieznanej komunikacji sieciowej dla ruchu przychodzącego i wychodzącego.
5. Jako domyślne akcje dla nieznanego ruchu sieciowego rozwiązanie pozwala określić blokowanie lub zezwolenie na taką komunikację.
6. Administrator posiada możliwość stworzenia reguł stosowanych w przypadku aktywacji izolacji hosta od sieci.

Kontrola www

1. Rozwiązanie posiada funkcję blokowania dostępu do kategorii witryn WWW skatalogowanych przez systemy reputacyjne producenta bez konieczności ręcznego wpisywania poszczególnych adresów.
2. Oprogramowanie zapewnia co najmniej 30 kategorii witryn WWW.
3. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
4. Rozwiązanie posiada możliwość blokowania witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.

Software updater

1. Rozwiązanie posiada wbudowany moduł aktualizacji aplikacji firm trzecich, który okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
2. Moduł aktualizacji aplikacji pełni rolę programu łatającego podatności i instalującego aktualizacje oprogramowania, a nie pasywnego skanera luk w bezpieczeństwie aplikacji.
3. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji.
4. Dodanie aplikacji wykluczonych z aktualizacji odbywa się na podstawie nazwy aplikacji, ID biuletynu oraz dostawcy aplikacji.
5. System centralnego zarządzania pozwala prezentować niezaktualizowane aplikacje na komputerach klienckich.
6. Mechanizm aktualizacji oprogramowania firm trzecich nie wymaga instalowania dodatkowych agentów oprócz agenta EPP.
7. Mechanizm aktualizacji oprogramowania firm trzecich pozwala na wymuszenie instalacji aktualizacji w sposób akcji wymuszonej z poziomu interfejsu zarządzania lub reguły harmonogramu wykonującej się w sposób zaplanowany konkretnego dnia i o konkretnej godzinie.
8. W przypadku gdy aktualizacja oprogramowania nie mogła się wykonać zgodnie z harmonogramem, zadanie instalacji może być uruchomione w najbliższym możliwym terminie z pominięciem harmonogramu.
9. W przypadku gdy aplikacja musi zostać zamknięta przed procesem aktualizacji administrator ma możliwość określenia czy ma się to odbyć automatycznie – bez wiedzy użytkownika, czy też ma się wyświetlić odpowiedni komunikat użytkownikowi z informacją o konieczności zamknięcia obecnie uruchomionej aplikacji wymagającej aktualizacji.
10. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
11. Administrator posiada możliwość skonfigurowania instalacji automatycznej aktualizacji

Kontrola nośników zewnętrznych

1. Oprogramowanie umożliwia blokowanie lub zezwalanie na dostęp do wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
2. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.
3. Rozwiązanie pozwala na nałożenie blokady zapisywania plików na zewnętrznych nośnikach pamięci (tryb tylko do odczytu).
4. Rozwiązanie pozwala na blokadę uruchamiania oprogramowania z dysków zewnętrznych, jednocześnie blokada ta umożliwia korzystanie z pozostałych danych zapisanych na takich dyskach.
5. Administrator jest informowany o podłączanych do chronionych systemów urządzeniach zewnętrznych.
6. Informacja o podłączanych urządzeniach zewnętrznych dotyczy wszystkich urządzeń lub tylko nowych.

Zaawansowana ochrona przed ransomware

1. Oprogramowanie posiada dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware.
2. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
3. Administrator posiada możliwość określenia folderów, które mają zostać objęte dodatkową ochroną przed modyfikacją.
4. Administrator posiada możliwość określenia domyślnej reakcji na próby modyfikowania plików w chronionych folderach zezwalając na taką modyfikację lub blokowanie.
5. Rozwiązanie posiada możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.

Dodatkowe funkcje

1. Instalator oprogramowania na stacji końcowej posiada możliwość sprawdzenia istnienia poprzednich wersji oprogramowania oraz oprogramowania uniemożliwiającego poprawne działanie klienta.
2. W przypadku znalezienia oprogramowania uniemożliwiającego poprawne działanie klienta, instalator informuje o tym fakcie użytkownika i w razie akceptacji pozwala usunąć takie oprogramowanie.
3. Administrator posiada możliwość zdefiniowania automatycznego procesu usuwania programowania uniemożliwiającego poprawne działanie klienta, bez informowania użytkownika końcowego.
4. Administrator posiada możliwość zablokowania deinstalacji aplikacji chroniącej przez użytkownika końcowego.
5. Deinstalacja aplikacji może odbyć się po podaniu hasła skonfigurowanego przez administratora.
6. Administrator ma możliwość granularnego zablokowania zmiany konfiguracji przez użytkownika końcowego dla poszczególnych modułów ochrony oraz dostępnych funkcji aplikacji chroniącej.

**Ochrona urządzeń Mac**

Ochrona antywirusowa komputerów komunikuje się z systemem centralnego zarządzania.

Oprogramowanie jest kompatybilne z następującymi systemami operacyjnymi:

* macOS 14 "Sonoma"
* macOS 13 "Ventura"
* macOS 12 "Monterey"
1. Oprogramowanie zapewnia ochronę plików w czasie rzeczywistym, skanowania zgodnie z ustalonym harmonogramem.
2. Pozwala na tworzenie wykluczeń ze skanowania.
3. Pozwala na aktywację mechanizmu zapory ogniowej.
4. Posiada moduł ochrony przeglądania stron internetowych

**Opis systemu centralnego zarządzania**

System centralnego zarządzania może być zainstalowany na wersjach serwerowych systemów Microsoft Windows lub Linux.

Instalacja sytemu centralnego zarządzania dla Microsoft Windows wspiera następujące wersje systemów operacyjnych:

* Windows Server 2012 (Essentials, Standard, Datacenter)
* Windows Server 2012 R2 (Essentials, Standard, Datacenter)
* Windows Server 2016 (Essentials, Standard, Datacenter)
* Windows Server 2019 (Essentials, Standard, Datacenter)
* Windows Server 2022 (Essentials, Standard, Datacenter)

Instalacja sytemu centralnego zarządzania dla Linux wspiera następujące 64 bitowe wersje systemów operacyjnych:

* AlmaLinux 8.5
* CentOS 7, 8
* CentOS Stream 8
* Debian GNU Linux 9, 10
* openSUSE Leap 43, 15
* Oracle Linux 8
* Red Hat Enterprise Linux 6, 7, 8
* SUSE Linux Enterprise Server 11, 12, 15
* SUSE Linux Enterprise Desktop 11, 12, 15
* Ubuntu 16.04, 18.04, 20.04
1. Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej.
2. Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi jest zaszyfrowana.
3. Rozwiązanie pozwala na scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta.
4. Administratorzy mają możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.
5. Centralna konsola administracyjna umożliwia przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy.
6. Rozwiązanie pozwala na tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach.
7. Rozwiązanie pozwala na import struktury drzewa z Microsoft Active Directory.
8. Rozwiązanie pozwala na tworzenie reguł synchronizacji z Microsoft Active Directory umożliwiających automatyczną synchronizację klientów z aktualnie istniejącymi grupami komputerów.
9. Rozwiązanie pozwala na tworzenie reguł powiadamiania o nowych, niezarządzanych klientach w Microsoft Active Directory.
10. Rozwiązanie pozwala na blokowanie wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników.
11. Rozwiązanie pozwala na zdefiniowania hasła do odinstalowania aplikacji.
12. Rozwiązanie pozwala na definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów.
13. Rozwiązanie posiada możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji.
14. Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania. Dane muszą być przesyłane do serwera zarządzania podczas kolejnego połączenia.
15. Rozwiązanie pozwala na konfigurację włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.
16. Rozwiązanie umożliwia administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki.
17. Rozwiązanie pozwala na eksport raportów z pracy systemu do pliku HTML.
18. Rozwiązanie daje możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich.
19. Rozwiązanie posiada dedykowany system raportowania dostępny przez przeglądarkę internetową umożliwiający podgląd statystyk dotyczących wykrytych wirusów, przeprowadzonych ataków, zainstalowanego oprogramowania oraz statystyk połączenia stacji klienckich.
20. System raportowania umożliwia wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora.
21. Zarządzanie zdarzeniami i raportowanie pozwala na natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania.
22. Rozwiązanie daje możliwość przekierowania alertów bezpośrednio do serwera Syslog.
23. Rozwiązanie umożliwia tworzenie wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).
24. Rozwiązanie umożliwia wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączania programu.
25. Wykonywanie automatycznej kopii bazy danych systemu zarządzania centralnego może odbywać się zgodnie z harmonogramem określonym przez administratora.
26. Administrator posiada możliwość określenia liczby kopii bazy danych, jaka będzie przetrzymywana przez automatyczny system tworzenia kopii zapasowej.
27. Rozwiązanie posiada możliwość wygenerowania danych diagnostycznych z podpiętych komputerów za pomocą konsoli zarządzającej.
28. Rozwiązanie posiada możliwość bezpośredniego pobrania z komputera danych diagnostycznych z poziomu konsoli zarządzającej.
29. Administrator posiada możliwość komentowania stosowanej konfiguracji stacji końcowych za pomocą notatek umieszczonych w interfejsie graficznym konsoli zarządzającej.
30. Konsola wyposażona jest w panel kontrolny zawierający podstawowe informacje dotyczące obecnego stanu chronionego środowiska.
31. System zarządzania pozwala na tworzenie profili w zależności od systemu operacyjnego i wersji wykorzystywanego w organizacji oprogramowania służącego ochronie.

**Rozszerzone wsparcie techniczne**

System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 24 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego resellera na okres do dnia 30.06.2026.

System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Resellera Producenta w języku polskim w zakresie:

* Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
* Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
* Doradztwo w zakresie konfiguracji.
* Zdalne wsparcie techniczne.
* Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
* Przygotowanie do zdalnej konfiguracji.
* Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
* Minimum 1 zdalna rekonfiguracja w związku ze zmianą środowiska lub wymagań użytkownika.
* Minimum raz w roku zdalny przegląd konfiguracji i logów wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
* Minimum raz w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Dla zapewnienia wysokiego poziomu usług świadczenie wsparcia technicznego rozwiązania musi być realizowane przez certyfikowanego inżyniera. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7.

**Oferent musi przedłożyć dokumenty:**

* Certyfikat inżynierski potwierdzony przez Producenta. **(dołączyć do oferty)**
* Oświadczenie Producenta rozwiązania, iż oferent posiada zasoby w postaci certyfikowanych inżynierów i jest gotów świadczyć usługi wsparcia technicznego na terenie Polski. **(dołączyć do oferty)**
* Certyfikat potwierdzający posiadany status partnerski, potwierdzony przez Producenta rozwiązania. **(dołączyć do oferty)**

**2. Dostawa licencji oprogramowania antywirusowego z modułem wykrywania i reagowania na podejrzane aktywności na urządzeniach końcowych – 96 szt. licencji ( w tym 11 serwerów (4 szt. fizyczne + 7 szt. wirtualnych)), na okres do dnia 30.06.2026 r., zgodnie z poniższymi wymaganiami**

Ochrona niżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli, znajdującej się na serwerach producenta, do której dostęp zapewniony jest przez przeglądarkę internetową.

Od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, do prawidłowego działania wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli znajdującej się na serwerach producenta oraz w przypadku ochrony rozwiązań chmurowych ich prawidłowe podłączenie z usługami dostawcy.

Rozwiązanie dla ochrony antywirusowej stacji roboczych i system EDR wspiera następujące systemy operacyjne:

* + Microsoft Windows 10
	+ Microsoft Windows 11
	+ macOS 15 Sequoia
	+ macOS 14 Sonoma
	+ macOS 13 Ventura

Rozwiązanie dla ochrony antywirusowej i system EDR dla systemów serwerowych wspiera następujące systemy operacyjne:

* Microsoft® Windows Server 2016 Standard
* Microsoft® Windows Server 2016 Essentials
* Microsoft® Windows Server 2016 Datacenter
* Microsoft® Windows Server 2016 Core
* Microsoft® Windows Server 2019 Standard
* Microsoft® Windows Server 2019 Essentials
* Microsoft® Windows Server 2019 Datacenter
* Microsoft® Windows Server 2019 Core
* Microsoft® Windows Server 2022 Standard
* Microsoft® Windows Server 2022 Essentials
* Microsoft® Windows Server 2022 Datacenter
* Microsoft® Windows Server 2022 Core

Wspierane przeglądarki internetowe do obsługi konsoli zarządzającej:

* Microsoft Edge
	+ Mozilla Firefox
	+ Google Chrome
	+ Safari

Zarówno konsola jak i oprogramowanie antywirusowe do ochrony stacji roboczych oraz serwerów oraz system EDR posiada polski interfejs użytkownika.

Ten sam agent zainstalowany na systemach Windows umożliwia rozbudowę funkcjonalności o mechanizm zarządzania ekspozycją na atak (Exposure Management) – aktywacja dodatkowych funkcji uzależniona jest tylko od posiadanej licencji, automatycznie aktywowana w momencie jej dodania i nie wymaga reinstalacji agenta w środowisku oraz posiadania osobnej konsoli zarządzającej.

Funkcjonalności systemu mogą różnić się w zależności od platformy na jakiej zainstalowany jest agent ze względu na ich ograniczenia, jednak chronione platformy są zarządzane z tej samej konsoli zarządzającej

# Opis technologii ochrony antymalware dla stacji roboczych i serwerów

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki wymienne, monitora ruchu http oraz modułu wykrywającego rootkity.
2. Rozwiązanie posiada wbudowany mechanizm ochrony przed zagrożeniami typu ransonmware.
3. Rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI)
4. Rozwiązanie umożliwia wybór plików do skanowania – wszystkich plików lub tylko plików o określonych rozszerzeniach.
5. W momencie wykrycia infekcji rozwiązanie automatycznie stara się wyleczyć plik, a jeśli nie jest to możliwe przenosi go do bezpiecznego folderu kwarantanny.
6. Rozwiązanie posiada możliwość ręcznej reakcji na wykryte zagrożenie, w takim przypadku pozwala na: wyleczenie pliku, usunięcie, przeniesienie do kwarantanny, zmiany nazwy, zablokowania.
7. Rozwiązanie chroni plik systemowy HOSTS przed nieautoryzowanymi zmianami.
8. Rozwiązanie posiada mechanizmy skanujące dyski sieciowe.
9. Skanowanie dysków sieciowych jest możliwe dla dowolnych operacji na takich zasobach lub tylko przy wykonywaniu znajdujących się tam plików.
10. Rozwiązanie posiada możliwość tworzenia wykluczeń dla mechanizmów ochrony w czasie rzeczywistym, w tym co najmniej dla: plików, folderów, procesów.
11. Rozwiązanie posiada mechanizm ochrony ruchu http chroniący użytkownika przed malware oraz phishingiem.
12. Istnieje możliwość stworzenia wykluczenia dla wskazanej aplikacji, tak aby nie skanowała ona ruchu http.
13. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
14. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
15. Rozwiązanie posiada możliwość dystrybuowania aktualizacji baz definicji wirusów oraz aktualizacji oprogramowania zainstalowanego na stacji końcowej, za pomocą serwera pośredniczącego.
16. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej do nowej wersji, następuje w sposób automatyczny, niewidoczny dla użytkownika końcowego.
17. Aktualizacja oprogramowania klienta zainstalowanego na stacji końcowej nie wymaga dodatkowych czynności konfiguracyjnych ze strony administratora systemu i następuje automatycznie w momencie udostępnienia takiej aktualizacji przez producenta.
18. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli zarządzania.
19. Rozwiązanie posiada możliwość wywołania procesu aktualizacji oprogramowania klienta zainstalowanego na stacji końcowej w określone dni i godziny tygodnia i miesiąca.
20. Rozwiązanie posiada możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów, za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
21. Rozwiązanie posiada możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
22. Rozwiązanie posiada możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
23. Rozwiązanie posiada możliwość wywołania skanowania uwzględnionych rozszerzeń a także ich wykluczanie.
24. Rozwiązanie posiada możliwość skanowania urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp.
25. Skanowanie dysków przenośnych może odbywać się w sposób automatyczny bez wiedzy użytkownika, automatycznie z wyświetleniem podsumowania skanowania użytkownikowi oraz z możliwością zablokowania opcji przerwania skanowania przez użytkownika końcowego.
26. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
27. Rozwiązanie posiada funkcję skanowania na żądanie pojedynczych plików, katalogów, napędów przy pomocy skrótu w menu kontekstowym
28. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
29. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
30. Rozwiązanie posiada heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
31. Umożliwia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”, „rootkit”.
32. Posiada mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), bazujący na technologii chmurowej, analizującej podejrzane pliki wykonywalne.
33. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń typu 0-day, technologia ta powinna w głównej mierze bazować na metadanych na temat analizowanego pliku. Pliki sklasyfikowane jako bezpieczne, nie są wysyłane do analizy w infrastrukturze producenta.
34. Rozwiązanie posiada technologię wykrywania nowych i nieznanych zagrożeń, która w przypadku podejrzanych plików umożliwia automatyczne ładowanie ich do systemu sandbox, utrzymywanego w infrastrukturze dostawcy oprogramowania antywirusowego w celu przeprowadzenia dodatkowej strukturalnej i behawioralnej analizy podejrzanego pliku.
35. Rozwiązanie posiada możliwość wyłączenia mechanizmu automatycznego przesyłania podejrzanych plików do dodatkowej analizy przez producenta.
36. Rozwiązanie posiada możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger”, „dialer”, „trojan” w kwarantannie.
37. Rozwiązanie posiada możliwość obsługi plików skompresowanych obejmującego najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.
38. Rozwiązanie posiada możliwość logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów jest możliwy z poziomu GUI aplikacji jak i konsoli centralnego zarządzania.
39. Rozwiązanie automatycznie powiadamia użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
40. Rozwiązanie posiada możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.
41. Rozwiązanie posiada możliwość wyłączenia interfejsu użytkownika oprogramowania zainstalowanego na stacji końcowej.
42. Rozwiązanie umożliwia blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.
43. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez system reputacyjny producenta.
44. Rozwiązanie posiada możliwość instalacji dodatku do przeglądarki internetowej (Google Chrome, Mozilla FireFox, MS Edge) pozwalającego na wyświetleniu graficznej informacji o reputacji witryny, która pojawia się w wynikach wyszukiwania w wyszukiwarkach internetowych.
45. Rozwiązanie jest wyposażone w mechanizm ochrony przeglądarki internetowej, w tym analizujący uruchamiane skrypty ActiveX i pobierane pliki.
46. Rozwiązanie posiada możliwość ochrony podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
47. Rozwiązanie umożliwia blokowanie dostępu do kategorii witryn WWW skatalogowanych przez systemy producenta.
48. Oprogramowanie zapewnia co najmniej 30 kategorii klasyfikacji witryn WWW.
49. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii, jest powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.
50. Rozwiązanie umożliwia blokowanie witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.
51. Rozwiązanie posiada wbudowany mechanizm zabezpieczenia połączenia do witryn skategoryzowanych przez producenta jako „bankowość elektroniczna”.
52. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie blokuje możliwość uruchamiania od strony chronionego hosta poleceń cmd oraz skryptów.
53. W momencie odwiedzania stron internetowych skategoryzowanych jako „bankowość elektroniczna” rozwiązanie automatycznie blokuje zdalny dostęp do hosta za pomocą takich narzędzi jak pulpit zdalny, TeamViewer, LogMein, VNC itp.
54. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora – administrator ma możliwość tworzenia własnej listy takich witryn.
55. Rozwiązanie posiada wbudowaną funkcję, która po zakończeniu sesji z witrynami sklasyfikowanymi jako „bankowość elektroniczna” czyści zawartość schowka systemowego.
56. Rozwiązanie posiada funkcję zarządzania zaporą ogniową (tzw. personal firewall) wbudowaną w system Windows, z opcją definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup.
57. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
58. Rozwiązanie pozwala na tworzenie własnych reguł w oparciu co najmniej o: kierunek komunikacji sieciowej, protokół sieciowy oraz możliwość wyboru akcji zezwolenia lub zablokowania wskazanej komunikacji.
59. Rozwiązanie posiada możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej).
60. Rozwiązanie umożliwia stworzenie zestawów reguł do natychmiastowego zastosowania, które zablokują komunikację sieciową w celu izolacji hosta na żądanie administratora.
61. Rozwiązanie jest wyposażone w mechanizm aktualizacji aplikacji (patch management), umożliwiający instalację dostępnych poprawek dla systemu operacyjnego oraz aplikacji na nim zainstalowanych.
62. Mechanizm aktualizacji aplikacji (patch management) nie wymaga instalowania dodatkowych agentów oprócz agenta AV.
63. Moduł aktualizacji aplikacji, okresowo skanuje aplikacje zainstalowane na stacji roboczej i umożliwia ich aktualizację do najnowszych wersji.
64. Moduł aktualizacji aplikacji pełni role mechanizmu łatającego podatności i instalującego aktualizacje oprogramowania, a nie jedynie pasywnego skanera luk w bezpieczeństwie aplikacji.
65. Administrator posiada możliwość określenia, kiedy i jakie aktualizacje mają zostać zainstalowane automatycznie.
66. Administrator posiada możliwość uruchomienia aktualizacji dla systemu operacyjnego jak i aplikacji znajdujących się na nim na żądanie dla wybranych lub wszystkich hostów.
67. Mechanizm aktualizacji aplikacji umożliwia automatyczne wyświetlenie komunikatu użytkownikowi od strony hosta o konieczności zamknięcia danej aplikacji, tak aby proces aktualizacji mógł się zakończyć.
68. W przypadku gdy instalacja aktualizacji dla systemu operacyjnego lub innej aplikacji wymaga restartu hosta w celu jej zastosowania, administrator posiada możliwość wymuszenia automatycznego restartu, wymuszenia restartu po określonej liczbie godzin, lub wyświetlenia komunikatu użytkownikowi o konieczności restartu.
69. Administrator konsoli zarządzającej ma możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.
70. Mechanizm aktualizacji aplikacji (patch management) nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.
71. Administrator ma możliwość zdefiniowania aplikacji, które nie podlegają aktualizacji, poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.
72. Rozwiązanie umożliwia wyświetlenie w GUI od strony chronionego hosta informacji o brakujących poprawkach dla systemu lub aplikacji i umożliwienie, ich instalacji przez użytkownika końcowego.
73. System centralnego zarządzania prezentuje niezaktualizowane aplikacje występujące na wszystkich chronionych hostach lub listę nieaktualizowanego oprogramowania dla pojedynczej stacji końcowej.
74. Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.
75. Mechanizm kontroli urządzeń zewnętrznych wspiera m.in. urządzenia takie jak: pamięci masowe, napędy CD/DVD, modemy, porty COM i LTP, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth.
76. Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej.
77. Lista urządzeń zaufanych jest tworzona co najmniej w oparciu o nazwę urządzenia i identyfikator sprzętowy.
78. Rozwiązanie posiada możliwość blokady zapisywania plików na zewnętrznych dyskach USB urządzenia takie są wówczas dostępne w trybie tylko do odczytu.
79. Mechanizm kontroli urządzeń umożliwia blokadę uruchamiania plików wykonywalnych z nośników pamięci. Blokada ta pozwala na korzystanie z pozostałych danych zapisanych na takich nośnikach.
80. Rozwiązanie posiada opcję zabezpieczenia hasłem możliwości deinstalacji agenta przez użytkownika końcowego.
81. Zmiany w konfiguracji mogą być dokonywane przez użytkownika końcowego tylko dla poszczególnych funkcji aplikacji wskazanych przez administratora w profilu.
82. Rozwiązanie posiada wbudowany mechanizm przywracania plików zaszyfrowanych przez zagrożenia typu ransomware.
83. Mechanizm w swoim działaniu wykorzystuje własną technologię producenta, nie inne technologie takie jak Volume Shadow Copy Service (VSS)
84. W przypadku wykrycia szkodliwego działania ransomware, moduł blokuje aktywność szkodliwego procesu oraz przywraca pliki, które zostały zaszyfrowane do oryginalnej formy i lokalizacji.
85. Moduł przywracania plików zaszyfrowanych może działać w trybie monitorowania, bez podejmowania reakcji.
86. Administrator ma możliwość wskazania własnego folderu, do którego będą kopiowane pliki tworzonej kopii zapasowej plików.
87. Administrator posiada możliwość określenia maksymalnej wielkości pliku, którego kopia zapasowa będzie tworzona przez moduł przywracania.
88. Rozwiązanie jest wyposażone w dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware niezależnie od pozostałych modułów ochrony. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.
89. Moduł posiada możliwość pracy w trybie monitorowania (bez blokowania) przekazując administratorowi informacje dotyczące prób modyfikacji plików w chronionych folderach.
90. Administrator posiada możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.
91. Istnieje możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną antyransomware.
92. Rozwiązanie potrafi automatycznie wykryć zaufane aplikacje, dla których będzie zezwolony dostęp do plików w chronionych folderach, oraz daje możliwość wskazania zaufanych aplikacji przez administratora.
93. Rozwiązanie posiada funkcjonalność kontroli uruchamianych aplikacji.
94. Tryb kontroli aplikacji umożliwia uruchomienie wszystkich aplikacji, uruchomienie i monitorowanie wszystkich aplikacji, blokowanie niezaufanych aplikacji
95. Istnieje możliwości blokowania, zezwolenia lub monitorowania aplikacji w oparciu, co najmniej o docelowy identyfikator SHA1,SHA256, lokalizację pliku, wersję pliku, nazwę aplikacji, wielkość pliku, wydawcę, ważność podpisu cyfrowego aplikacji.
96. Tworzone reguły dotyczyć mogą czynności: uruchomienia aplikacji, ładowania modułu, uruchomienia instalatora, dostępu do pliku.
97. Na wspieranych systemach Windows rozwiązanie pozwala na zdalne wywołanie procesu szyfrowania za pomocą funkcji BitLocker wbudowanej w system operacyjny.
98. Administrator posiada w momencie konfiguracji procesu szyfrowania, możliwość wymuszenia od strony użytkownika ustanowienia dodatkowego zabezpieczenia w postaci kodu PIN
99. Rozwiązanie posiada możliwość przekazywania do konsoli administracji zdalnej kluczy odzyskiwania funkcji BitLocker
100. Rozwiązanie pozwala na zdalne uruchomienie procesu deszyfrowania wcześniej zaszyfrowanych dysków systemowych.
101. Administrator w konsoli zarządzającej posiada dostępne informacje dotyczące stanu zaszyfrowania dysków systemowych.
102. Rozwiązanie pozwala na uzyskiwanie informacji pochodzących z dziennika systemu Windows dotyczących między innymi: Czyszczenia dziennika audytu, zablokowania konta użytkownika, utworzenia konta użytkownika, zmiany konta użytkownika, błędnych prób logowania użytkownika, wystąpienia błędu krytycznego (BSOD)
103. Administrator ma możliwość wyboru, które z informacji pochodzących z dziennika systemu Windows mają być przekazywane do konsoli zarządzającej.
104. Rozwiązanie pozwala na wygenerowanie pliku za pocą którego administrator może wywołać zdalne podłączenie za pomocą usług Microsoft RDP (Remote Desktop).
105. Wygenerowany plik może być otwarty i wykorzystany do zdalnego podłączenia za pomocą Microsoft Terminal Services Client (MSTSC), Microsoft Remote Desktop i innych wspierających usług i aplikacji.

#### **Opis technologi Endpoint Detection and Response (EDR) dla stacji roboczych i serwerów**

1. Dane zebrane przez agenta instalowanego na stacjach końcowych są przesyłane w trybie ciągłym, szyfrowanym protokołem HTTPS, do centrum przetwarzania danych producenta, w celu wykrywania niebezpiecznych zdarzeń.
2. Agent instalowany na stacjach końcowych i serwerach monitoruje i zbiera informacje na temat co najmniej następujących zdarzeń:
	* dostęp do pliku;
	* tworzenie nowego procesu;
	* nawiązane połączenia sieciowe;
	* wpisy dziennika systemu, niezbędne do wykrycia naruszeń bezpieczeństwa;
	* zawartość skryptów uruchamianych na monitorowanej stacji.
3. W celu zmniejszenia obciążenia stacji końcowych wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywają się w centrum przetwarzania danych producenta, a nie na monitorowanej stacji końcowej.
4. Dane zbierane przez agenta instalowanego na stacjach końcowych, przed wysłaniem do centrum przetwarzania danych, są kompresowane w celu optymalizacji wykorzystania łączy sieciowych.
5. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, z centrum przetwarzania danych producenta, odbywa się jedynie z wykorzystaniem protokołów HTTP oraz HTTPS.
6. Komunikacja agentów instalowanych na stacjach roboczych i serwerach, wspiera komunikację za pomocą serwera pośredniczącego http (http proxy).
7. W przypadku braku dostępu do sieci Internet, na monitorowanej stacji, która skutkuje brakiem możliwości przesłania danych zebranych przez agenta do centrum przetwarzania danych producenta, dane zebrane na stacji końcowej są buforowane i przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.
8. Dane zbierane przez agentów na stacjach końcowych i serwerach są, przechowywane i przetwarzane na obszarze Europejskiej Wspólnoty Gospodarczej.
9. Rozwiązanie na bazie zebranych danych generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji roboczych i serwerów.
10. Detekcje są generowane za pomocą statycznych reguł, przygotowanych przez producenta, jak również przy wykorzystaniu mechanizmów uczenia maszynowego uwzględniających specyfikę pracy środowiska informatycznego.
11. Detekcje są generowane w czasie rzeczywistym na podstawie danych zebranych i przesłanych przez agentów uruchomionych na stacjach końcowych i serwerach w środowisku informatycznym.
12. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów, przedstawiających wykryte anomalie i powiązania pomiędzy biorącymi udział w detekcji elementami.
13. Rozwiązanie posiada możliwość filtrowania zdarzeń biorących udział w detekcji w zależności od poziomu ryzyka – od poziomu informacyjnego do zdarzeń o charakterze krytycznym.
14. Każda detekcja zawiera co najmniej następujące informacje:
	* Lista urządzeń na których rozwiązanie zarejestrowało podejrzane zdarzenia.
	* Data i czas wystąpienia podejrzanych zdarzeń.
	* Listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie.
	* Opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane.
	* Sumę kontrolną (co najmniej SHA1) plików, które zostały uznane za podejrzane.
	* Poziom ryzyka, określający istotność danej detekcji.
	* Typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu).
15. Zdarzenia, występujące w detekcjach, które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK).
16. Zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal).
17. Rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędne.
18. Oznaczenie detekcji jako błędnej, musi powodować, automatyczne identyfikowanie przyszłych takich samych detekcji i odpowiednie ich oznaczenie w interfejsie centralnego zarządzania.
19. Rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące hosta, na którym wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
20. Rozwiązanie pozwala na dodanie własnego komentarza przy wykrytej detekcji.
21. Rozwiązanie umożliwia wykupienie usługi pozwalającej na przesłanie detekcji do laboratorium producenta w celu analizy, zwrotnie administrator otrzymuje szczegółowy raport przygotowany przez analityka dotyczący incydentu.
22. Rozwiązanie pozwala na przesłanie wiadomości e-mail informującej o wygenerowaniu nowej detekcji w systemie.
23. Rozwiązanie pozwala na izolację sieciową komputerów przez administratora.
24. Rozwiązanie umożliwia tworzenie reguł automatycznej izolacji stacji roboczych i serwerów, jeśli zostaną one uwzględnione w wygenerowanych detekcjach.
25. Rozwiązanie umożliwia wykonanie zdalnie reakcji na chronionym hoście w tym co najmniej pozwala na: pobranie plików, pobranie historii PowerShell, pobranie wpisów dziennika zdarzeń, pobranie dziennika ochrony antywirusowej, pobranie informacji o wpisach rejestru systemowego, pobranie informacji o MBR, wylistowanie procesów, wylistowanie informacji z systemowego harmonogramu zadań, wylistowanie usług, umożliwia zatrzymanie procesu lub wątku, umożliwia usuwanie plików, usług, wartości rejestru systemowego oraz zadań systemowego harmonogramu zadań.
26. Rozwiązanie umożliwia tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
27. Rozwiązanie pozwala na eksport raportów, w postaci plików PDF.
28. Rozwiązanie wspiera dostęp do danych na temat utworzonych detekcji za pomocą interfejsu REST API, na potrzeby integracji z innymi systemami zabezpieczającymi.
29. Rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: PID nowego procesu, SHA-1 nowego procesu, nazwę procesu, ścieżkę, nazwę procesu docelowego, docelową ścieżkę, typ zdarzenia, nazwę systemu, typ systemu, wersję systemu, adres IP źródłowy oraz zdalny, port lokalny oraz port zdalny, wartość klucza rejestru.
30. Konsola wyposażona w dedykowaną zakładkę zawierającą listę urządzeń posiadających zainstalowanego agenta systemu EDR.
31. Lista urządzeń posiadających zainstalowanego agenta systemu EDR zawiera informacje dotyczące: nazwy hosta, adresu IP, poziomu ważności, przypisanego profilu, systemu operacyjnego, informacji o ostatnim podłączeniu oraz aktualnym statusie.
32. Rozwiązanie posiada wbudowane narzędzie pozwalające na stworzenie podsumowania incydentu na podstawie dostępnych danych.
33. Narzędzie umożliwiające stworzenie podsumowania incydentu w swoim działaniu wykorzystuje mechanizmy sztucznej inteligencji.
34. Generowane podsumowanie incydentu dostępne jest w języku wykorzystywanym w konsoli zarządzającej.
35. Rozwiązanie pozwala na wykupienie dodatkowych usług monitorowa oraz monitorowania i reakcji (MDR) na incydenty dla systemu EDR, które realizowane są przez zespoły bezpieczeństwa producenta rozwiązania.
36. Wykupienie usługi nie ogranicza administratorowi dostępu do konsoli zarządzającej i nie wymaga reinstalacji agentów.

**Opis technologii monitorowania podejrzanej aktywności na poziomie kont MS Entra ID**

1. Rozwiązanie pozwala na synchronizację z usługami Entra ID
2. Rozwiązanie w przypadku wykrycia podejrzanie aktywności kont monitorowanych na poziomie Entra ID generuje detekcję widoczną w konsoli.
3. Wygenerowana detekcja posiada: ID Detekcji, określony poziom krytyczności, datę detekcji, datę ostatniej modyfikacji, status, informacje o dodanym komentarzu.
4. Administrator posiada możliwość wglądu w szczegóły danej detekcji.
5. W ramach szczegółów detekcji administrator ma możliwość manualnego określenia statusy detekcji, w zależności od etapu jej analizy.
6. Administrator posiada informacje dotyczące źródła detekcji, organizacji, dla której detekcja została wygenerowana, zasobu oraz lokacji dotkniętej wykrytą podejrzana aktywnością.
7. W ramach szczegółów detekcji administrator otrzymuje jej podsumowanie, opis, informacje o ryzyku z jakim związana jest dana aktywność oraz sugerowane rekomendacje.

**Opis technologii ochrony dla usług Microsoft 365**

1. Rozwiązanie służy ochronie antymalware dla pakietu Microsoft 365 na poziomie ochrony usług poczty email MS Exchange, usługi MS Sharepoint, usługi MS OneDrive oraz MS Teams.
2. Rozwiązanie integruje się bezpośrednio z usługami firmy Microsoft bez konieczności instalacji dodatkowych serwerów pośredniczących w środowisku klienta.
3. Konfiguracja połączenia z usługami Microsoft odbywa się za pomocą kreatora.
4. Rozwiązanie pozwala na określenie czy ochroną mają być objęte wszystkie konta pocztowe na wskazanej usłudze czy też tylko te wskazane przez administratora.
5. Rozwiązanie pozwala na tworzenie polityk konfiguracyjnych, które administrator może przypisać do poszczególnych usług.
6. W przypadku ochrony usług Microsoft Exchange rozwiązanie pozwala na aktywację mechanizmów ochrony antymalware w czasie rzeczywistym dla wiadomości przychodzących.
7. Rozwiązanie pozwala na tworzenie białych list dla konkretnych adresów email oraz domen.
8. Rozwiązanie pozwala na określenie czasu, po którym obiekty poddane kwarantannie zostaną usunięte, w tym po 1 miesiącu, 3 miesiącach, 6 miesiącach, 1 roku.
9. Rozwiązanie pozwala na określenie czy skanowane mają być wszystkie typy plików czy też tylko pliki o określonych rozszerzeniach.
10. Rozwiązanie pozwala na skanowanie wewnątrz plików archiwów.
11. W przypadku podejrzanych obiektów rozwiązanie pozwala na automatyczną detonację plików w usłudze sandboxingu hostowanej w infrastrukturze producenta.
12. W przypadku wykrycia zagrożenia rozwiązanie pozwala na: przeniesienie obiektu do kwarantanny, poddanie kwarantannie jedynie szkodliwego załącznika, usunięciu całej wiadomości, usunięciu jedynie załącznika lub pozostawieniu obiektu.
13. Rozwiązanie pozwala na wysyłanie powiadomień na wskazane adresy email w przypadku wykrycia zagrożenia.
14. Rozwiązanie pozwala na spersonalizowanie wiadomości wysyłanej w momencie wykrycia zagrożenia.
15. Rozwiązanie pozwala na skanowanie adresów URL pod kątem szkodliwej zawartości.
16. W przypadku wykrycia szkodliwego adresu URL rozwiązanie pozwala na przeniesienie obiektu zawierającego szkodliwy adres URL do kwarantanny, usunięcia obiektu, zmianę tematu wiadomości oraz od linkowanie adresu URL w celu zapobiegania przypadkowemu kliknięciu przez użytkownika.
17. W przypadku wykrycia szkodliwego adresu URL rozwiązanie może informować administratora poprzez wysłanie powiadomienia o tym fakcie na wskazany adres email
18. Rozwiązanie pozwala na wykrywanie podejrzanych adresów URL
19. W przypadku wykrycia podejrzanego adresu URL rozwiązanie pozwala na przeniesienie obiektu zawierającego szkodliwy adres URL do kwarantanny, usunięcia obiektu, zmianę tematu wiadomości oraz od linkowanie adresu URL w celu zapobiegania przypadkowemu kliknięciu przez użytkownika.
20. Rozwiązanie pozwala na personalizację tematu wiadomości jaki pojawi się w momencie, gdy podejrzana zawartość zostanie wykryta przez mechanizmy skanujące.
21. Rozwiązanie pozwala na tworzenie listy zaufanych adresów URL dla których skanowanie nie będzie wykonywane
22. Rozwiązanie pozwala na tworzenie listy zablokowanych adresów URL dla których dostęp będzie automatycznie blokowany.
23. Rozwiązanie pozwala na skanowanie reguł wykorzystywanych dla poczty przychodzącej na poziomie kont użytkownika, w tym: podejrzanej nazwy reguły, podejrzanego przenoszenia wiadomości email, podejrzanego usuwania wiadomości email, podejrzanego przekazywania wiadomości email.
24. Rozwiązanie posiada funkcjonalność monitorującą chronione konta email pod kątem pojawienia się ich w wyciekach danych.
25. Rozwiązanie w momencie wykrycia faktu pojawienia się adresu email chronionego konta w wycieku danych informuje o tym fakcie administratora.
26. W momencie wykrycia faktu pojawienia się objętego ochroną adresu email w wycieku danych, administrator uzyskuje informacje dotyczące: adresu email, który pojawił się w wycieku danych, źródła wycieku, informacji o tym w jakiej formie wyciekło hasło oraz informacji dotyczące ostatniej zmiany hasła dla chronionego konta email.
27. Rozwiązanie posiada mechanizm zarządzania kwarantanną umożliwiający uzyskanie informacji na temat obiektu poddanego kwarantannie w tym: jego źródła, odbiorcy, do którego skierowana była szkodliwa zawartość, typu obiektu jaki został określony jako szkodliwy
28. Mechanizm kwarantanny pozwala administratorowi na wgląd w szczegóły detekcji.
29. Administrator posiada możliwość usunięcia obiektu poddanego kwarantannie oraz jego uwolnienia z kwarantanny.
30. Rozwiązanie posiada możliwość generowania raportów zgodnie z harmonogramem, w tym dziennie, tygodniowo, miesięcznie.
31. Raporty dostępne są w postaci plików PDF
32. Rozwiązanie pozwala na skanowanie plików przesyłanych do objętej ochroną instancji MS Sharepoint wchodzącej w skład pakietu Microsoft 365.
33. Rozwiązanie pozwala na skanowanie wszystkich typów plików, plików o określonych rozszerzeniach lub wszystkich typów plików poza wykluczonymi przez administratora.
34. Rozwiązanie pozwala na skanowanie plików archiwów.
35. W przypadku podejrzanych obiektów rozwiązanie pozwala na automatyczną detonację plików w usłudze sandboxingu hostowanej w infrastrukturze producenta.
36. W przypadku wykrycia szkodliwego obiektu na chronionej instancji MS Sharepoint wchodzącej w skład pakietu usług Microsoft 365 rozwiązanie pozwala na poddanie pliku kwarantannie, jego usunięcie lub niewykonywanie akcji.
37. Rozwiązanie pozwala na skanowanie plików przesyłanych do objętej ochroną instancji MS OneDrive wchodzącej w skład pakietu Microsoft 365.
38. Rozwiązanie pozwala na skanowanie wszystkich typów plików, plików o określonych rozszerzeniach lub wszystkich typów plików poza wykluczonymi przez administratora.
39. Rozwiązanie pozwala na skanowanie plików archiwów.
40. W przypadku podejrzanych obiektów rozwiązanie pozwala na automatyczną detonację plików w usłudze sandboxingu hostowanej w infrastrukturze producenta.
41. W przypadku wykrycia szkodliwego obiektu na chronionej instancji MS OneDrive wchodzącej w skład pakietu usług Microsoft 365 rozwiązanie pozwala na poddanie pliku kwarantannie, jego usunięcie lub niewykonywanie akcji.
42. Rozwiązanie pozwala na skanowanie obiektów dostępnych na platformie MS teams w ramach organizacji

**Centralna administracja**

1. Portal zarządzający jest dostępny w języku polskim.
2. Poza językiem polskim konsola wspiera języki: angielski, niemiecki, francuski, hiszpański, fiński, włoski.
3. Logowanie do konsoli umożliwia wykorzystanie mechanizmów wieloskładnikowego uwierzytelniania (2FA) dla kont posiadających dostęp do konsoli zarządzającej.
4. Mechanizm 2FA służący zabezpieczeniu dostępu do konsoli zarządzającej w swoim działaniu wykorzystuje mechanizmy: powiadomień SMS, oraz tokenów jednorazowych generowanych w aplikacjach mobilnych (np. Google Authenticator, Microsoft Authenticator).
5. Komunikacja pomiędzy portalem centralnego zarządzania a stacjami roboczymi odbywa się w formie zaszyfrowanej.
6. W celu korzystania z centralnej administracji, od strony chronionego środowiska nie jest wymagana instalacja dodatkowych elementów takich jak: baza danych, serwer http, serwery proxy, wymagana jest jedynie instalacja agenta na wspieranych końcówkach, które łączą się do centralnej konsoli zarządzającej znajdującej się na serwerach producenta.
7. Interfejs zarządzania posiada funkcję wyświetlania monitów o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.
8. Interfejs jest wyposażony w panel kontrolny zawierający podsumowanie stanu bezpieczeństwa organizacji w postaci graficznych wykresów.
9. Wykresy są interaktywne, tzn., że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe dane menu.
10. Rozwiązanie posiada dedykowaną zakładkę zawierającą informację o wszystkich hostach posiadających zainstalowane oprogramowanie do ochrony, w tym: ich nazwy, status ochrony, przypisany profil bezpieczeństwa.
11. Istnieje możliwość eksportu listy wszystkich hostów do pliku CSV.
12. Administrator ma możliwość wglądu w szczegóły zgłaszającego się hosta, w których zawarte są informacje dotyczące: ostatniego podłączenia do konsoli zarządzającej, wersji zainstalowanego produktu, systemu operacyjnego, stanu ochrony, akcji związanych z wykrytymi zagrożeniami i skanowaniami.
13. Administrator ma możliwość z poziomu szczegółów klienta, uruchomienia skanowania antywirusowego, instalacji aktualizacji dla aplikacji i systemu operacyjnego, przypisania profilu, usunięcia urządzenia, zmiany klucza subskrypcji, odizolowania hosta od sieci i pobrania pliku diagnostycznego.
14. Komputery nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie - co najmniej 60 dni.
15. Rozwiązanie posiada dodatkową zakładkę zawierającą informacje dotyczącą brakujących aktualizacji dla zainstalowanych aplikacji i systemu operacyjnego.
16. Istnieje możliwość posortowania i filtrowania brakujących poprawek pod względem ich poziomu krytyczności.
17. Informacje dotyczące brakujących poprawek dla aplikacji i systemu operacyjnego zawierają liczbę i typ hostów, na których został wykryty brak danej poprawki.
18. Po wskazaniu danej poprawki administrator posiada możliwość jej instalacji na wskazanych komputerach lub na wszystkich komputerach i serwerach, dla których dana poprawka została wydana.
19. Administrator ma możliwość wglądu w historię instalowanych poprawek na chronionych hostach.
20. Rozwiązanie posiada moduł raportujący w którym wyświetlane są informacje dotyczące stanu ochrony, infekcji malware, instalowanych aplikacji.
21. Raporty mogą być tworzone zgodnie z harmonogramem i wysyłane na wskazane adresy email.
22. Rozwiązanie posiada wbudowany mechanizm zarządzania subskrypcjami, z możliwością dodawania nowych kluczy licencyjnych.
23. Administrator widzi w konsoli informacje dotyczące produktu na jaki posiada licencję, klucz licencyjny, typy licencji, wykorzystanie oraz daty wygaśnięcia licencji.
24. Portal zarządzający umożliwia dodawanie kluczy licencyjnych dla innych produktów w celu aktywacji danej funkcjonalności.
25. Dodanie klucza licencyjnego skutkuje aktywacją zawartości dedykowanej zakładki obsługującej dany produkt w portalu zarządzającym.
26. Rozwiązanie ma możliwość definiowania różnych profili ustawień dla chronionych urządzeń z poziomu portalu zarządzającego.
27. Profile mogą być przypisane do pojedynczych hostów lub do grup.
28. Profile mogą być automatycznie przypisywane do hostów spełniających określone warunki w tym: adresy IP, DNS, nazwa WINS, przynależność do AD.
29. W przypadku automatycznego przypisywania profili, system pozwala na automatyczne dodawanie tagów dla hostów które otrzymają dany profil konfiguracyjny.
30. Istnieje możliwość porównania 2 profili konfiguracyjnych w celu wyświetlenia różnic pomiędzy nimi.
31. Rozwiązanie pozwala administratorowi podczas tworzenia profili wskazanie funkcjonalności, które mogą być zmieniane przez użytkownika od strony chronionego hosta – możliwość wprowadzanych zmian jest do określenia dla poszczególnych funkcji programu oraz całości konfiguracji.
32. Z poziomu portalu zarządzającego istnieje możliwość pobrania plików instalacyjnych, wykorzystywanych do instalacji agenta na objętych licencją hostach.
33. Pliki instalacyjne mają posiadać plików .EXE, .MSI .MPKG, .DEB, .RPM w zależności od platformy i typu systemu na jakich ma zostać zainstalowany agent.
34. Tworzone profile muszą dają administratorowi możliwość blokowania ustawień konfiguracyjnych aplikacji zainstalowanych od strony stacji roboczych w celu uniemożliwienia ich modyfikacji przez lokalnego użytkownika.
35. Administrator posiada możliwość wyświetlenia dodatkowych szczegółów dotyczących chronionych hostów.
36. Administrator posiada do wyboru ponad 100 różnych dodatkowych informacji, które mogą być widoczne w tym co najmniej: wersji BIOS, identyfikatora CPU, ilości rdzeni procesora, wolnej ilości miejsca na dysku, informacji o fakcie wykorzystania systemu operacyjnego Windows który osiągnął cykl end of life, aktywnego wygaszacza ekranu, zalogowanego konta administracyjnego.
37. Portal zarządzający pozwala na zarządzanie oprogramowaniem instalowanym na urządzeniach mobilnych (smartphony) w przypadku posiadania odpowiedniej licencji.
38. Konsola posiada możliwość definiowania wielu kont administratorów o różnych poziomach dostępu.
39. W ramach posiadanych licencji istnieje możliwość przenoszenia oprogramowania w ramach danego klucza subskrypcji z jednej stacji roboczej na inną.
40. Konsola posiada wbudowane narzędzie umożliwiające wygenerowanie podsumowania zdarzeń bezpieczeństwa z okresu ostatnich 7 dni.
41. Narzędzie w swoim działaniu wykorzystuje mechanizmy sztucznej inteligencji.
42. Wygenerowane podsumowanie zdarzeń bezpieczeństwa dostępne jest w języku wykorzystywanym w konsoli
43. Korzystanie z narzędzia nie wymaga posiadania dodatkowej licencji.

**Rozszerzone wsparcie techniczne**

System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 24 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego resellera na okres do dnia 30.06.2026.

System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Resellera Producenta w języku polskim w zakresie:

* Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
* Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
* Doradztwo w zakresie konfiguracji.
* Zdalne wsparcie techniczne.
* Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
* Przygotowanie do zdalnej konfiguracji.
* Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
* Minimum 1 zdalna rekonfiguracja w związku ze zmianą środowiska lub wymagań użytkownika.
* Minimum raz w roku zdalny przegląd konfiguracji i logów wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
* Minimum raz w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Dla zapewnienia wysokiego poziomu usług świadczenie wsparcia technicznego rozwiązania musi być realizowane przez certyfikowanego inżyniera. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7.

**Oferent musi przedłożyć dokumenty:**

* Certyfikat inżynierski potwierdzony przez Producenta rozwiązania. **(dołączyć do oferty)**
* Oświadczenie Producenta rozwiązania, iż oferent posiada zasoby w postaci certyfikowanych inżynierów i jest gotów świadczyć usługi wsparcia technicznego na terenie Polski. **(dołączyć do oferty)**
* Certyfikat potwierdzający posiadany status partnerski, potwierdzony przez Producenta rozwiązania. **(dołączyć do oferty)**