Specyfikacja oprogramowania

Opis wymagań na oprogramowanie antywirusowe oraz zarządzane centralne:

Konsola zarządzająca

1. Konsola web administratora powinna znajdować się w chmurze producenta znajdującej się na terenie Unii Europejskiej i zapewniać możliwość pełnego zarządzania stacjami roboczymi/serwerami przez przeglądarkę Web, która ma dostęp do Internetu.

2. Konsola web administratora musi posiadać możliwość wyboru języka polskiego, jako język całego interfejsu.

3. Konsola web musi umożliwiać zarządzanie stacjami roboczymi oraz serwerami i urządzeniami mobilnymi poprzez tą samą konsolę zarządzającą.

4. Konsola web musi posiadać możliwość tworzenia grup i polityk dla stacji.

5. Administrator musi mieć możliwość przeniesienia z poziomu konsoli aktywnej licencji na inną stację roboczą, urządzenia mobilne, bądź serwer bez utraty ważności licencji.

6. Administrator musi mieć możliwość zarządzania kluczem licencyjnym z poziomu konsoli administracyjnej.

7. Konsola web musi umożliwiać bezpieczne logowanie do konsoli zarządzającej po protokole HTTPS z certyfikatem.

8. Konsola web musi umożliwiać dwuetapową autoryzację logowania na minimum 2 sposoby.

9. Konsola web musi posiadać możliwość zablokowania dostępu do ustawień programu ochrony dla użytkowników na urządzeniach nieposiadających uprawnień administracyjnych.

10. Konsola web musi posiadać funkcję, która uniemożliwia użytkownikowi komputera wyłączenie działania monitora antywirusowego i innych składników ochrony, jeżeli nie posiada uprawnień administratora.

11. Konsola web musi posiadać narzędzie do wykonania instalacji oprogramowania na stacjach poprzez Active Directory, grupy robocze lub zakresy adresów sieciowych IP.

12. Konsola web musi umożliwiać wykonanie instalacji oprogramowania firm trzecich zdalnie z konsoli na stacjach.

13. Konsola web musi umożliwiać geolokalizację z aktualną mapą urządzeń mobilnych iOS/Android wyposażonych w moduł GPS.

14. Konsola web musi mieć możliwość zdefiniowana zalecanych aplikacji, które może pobrać użytkownik urządzeń mobilnych.

15. Konsola web umożliwia usuwanie aplikacji z urządzeń mobilnych.

16. Konsola web musi umożliwiać wyczyszczenie lub zablokowanie zdalne urządzenia mobilnego.

17. Konsola web musi mieć możliwość zalogowania się kilku administratorom jednocześnie.

18. Konsola web powinna oferować predefiniowane domyślne ustawienia rekomendowanych polityk (ustawień) dla stacji końcowych.

19. Konsola web musi mieć funkcję planowania zadań, w tym planowania terminów automatycznego skanowania.

20. Konsola web umożliwia zmianę ustawień priorytetu skanowania.

21. Konsola web umożliwia wysyłanie powiadomień o zdarzeniach na wskazany adres mailowy.

22. Konsola web musi posiadać możliwość uruchamiania komputerów zdalnie (WakaOnLAN), uruchamiania ponownego oraz wyłączania urządzeń z systemem Windows.

23. Konsola web musi umożliwiać synchronizację z Azure Active Directory.

24. Konsola web musi obsługiwać moduł do odbierania zgłoszeń serwisowych od użytkowników bezpośrednio z stacji klienckiej.

25. Rozwiązanie musi posiadać dedykowanego aplikację lub stronę internetową do zgłoszeń serwisowych bez konieczności instalacji ochrony antywirusowej.

26. Konsola web musi posiadać zintegrowany moduł CRM z możliwością zaplanowania prac u użytkownika.

27. Konsola web musi posiadać moduł uruchamiania procedur (skrypty) zdefiniowanych przez producenta oraz przez użytkownika w języku Python.

Zarządzanie aktualizacjami

1. Oprogramowanie web musi zawierać zintegrowaną funkcjonalność menadżera aktualizacji (Patch Manager), który umożliwia zarządzanie pobieraniem aktualizacji (updatów) systemu Windows, Java, Adobe i innych producentów trzecich.

2. Producent powinien posiadać własne bezpieczne i sprawdzone repozytorium aplikacji do celów aktualizacji oprogramowania firm trzecich minimum 50 producentów.

Zarządzanie użytkownikami i stacjami

1. Rozwiązanie musi umożliwiać bezpośrednio z konsoli zarządzającej web uruchamianie procedur (skryptów) serwisowych na stacjach klienckich o minimalnych,następujących funkcjonalnościach:
-Czyszczenie plików tymczasowych,
-Czyszczenie i sprawdzanie dysku,
-Usuwanie błędów dysku,
-Defragmentowanie dysku,
-Czyszczenie kolejki drukarki,
-Czyszczenie pamięci podręcznej DNS,
-Czyszczenie kosza,
-Sprawdzanie błędów na dysku twardym S.M.A.R.T. Check,
-Włączenie szyfrowania dysku funkcją Bitlocker dla systemu Windows.

2. System powinien przyjmować zgłoszenia serwisowe bezpośrednio z agenta na stacji, pocztą email oraz po przez dedykowaną stronę dla działu serwisu.

3. System musi umożliwiać przydzielanie zgłoszenia serwisowego dla konkretnego administratora oraz powinien mieć zintegrowany system diagnozy stacji oraz możliwość podłączenia się poprzez zdalny pulpit.

4. Konsola web musi posiadać zintegrowany moduł umożliwiający zdalne połączenie z graficznym pulpitem zdalnym przez dedykowaną aplikację dla komputerów/serwerów znajdujących się w sieci LAN i poza nią bez potrzeby tworzenia tuneli VPN każdej stacji komputera/serwera/Windows.

5. Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do użytkowania przez administratora w określonym przez niego czasie.

6. Możliwość wyświetlania komunikatu przed połączeniem zdalnym pulpitem do użytkowania przez administratora w celu odpytania go o zgodę na połączenie.

7. Konsola web musi mieć funkcję tworzenia raportów o stacjach w konsoli.

8. Konsola web musi mieć funkcję logów wykonywanych czynności przez administratorów konsoli.

Agent ochrony konsoli – oprogramowanie antywirusowe

1. Program antywirusowy powinien mieć obsługę w języku polskim. Platforma powinna obsługiwać systemy operacyjne:

Android	**iOS**
4.x	7.x
4.x (KNOX)	8.x
5.x	9.x
5.x (KNOX)	10.x
6.x (KNOX)	11.x
7.x	12.x
7.x (KNOX)	13.x
8.x	14.x
8.x (KNOX)	15.x
9.x	
9.x (KNOX)	
10.x	**macOS**
10.x (KNOX)	
11.x	10.12.x
11.x (KNOX)	10.13.x
12.x	10.14.x
12.x (KNOX)	10.15.x
	11.x
	12.x

Windows (workstation edition)

Windows XP (SP3 or higher) x86
Windows 7 SP1 x86
Windows 7 SP1 x64
Windows 8 x86
Windows 8 x64
Windows 8.1 x86
Windows 8.1 x64
Windows 10 x86
Windows 10 x64
Windows 11 x64

Windows (wersja serwerowa)

Windows Server 2003 SP2
Windows Server 2003 R2 SP2
Windows Server 2008 SP2
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019

LinuxOS z gwarantowaną kompatybilnością:

Wersje systemu operacyjnego, na których produkt jest testowany i obsługiwany.

Latest Ubuntu 16.x LTS x64 release version (with GUI)
Latest Ubuntu 18.x LTS x64 release version (with GUI)
Latest Ubuntu 19.x x64 release version (with GUI)
Latest Ubuntu 20.x LTS x64 release version (with GUI)
Latest Ubuntu 21.04 x64 release version (with GUI)
Latest Debian 8.x x64 release version (with GUI)
Latest Debian 9.x x64 release version (wit
GUI)
Latest Debian 10.x x64 release version (with GUI)
Latest Red Hat Enterprise Linux Server 7.x x64 release version (with GUI)
Latest Red Hat Enterprise Linux Server 8.x x64 release version (with GUI)
Latest CentOS 7.x x64 release version (with GUI)
Latest CentOS 8.x x64 release version (with GUI)

2. Rozwiązanie powinno działać na komputerach wyposażonych minimalnie w:
-512 MB dostępnej pamięci RAM,
-1 GB miejsca na dysku twardym dla wersji 32-bitowej i 64-bitowej.

3. Instalacja oprogramowania musi być możliwa poprzez Active Directory, grupy robocze, poprzez sieć, pobranie paczki MSI i za pomocą dystrybucji przez pocztę e-mail.

4. Ochrona poczty - antywirus musi chronić stacje poprzez uruchamianie nieznanych oraz niebezpiecznych załączników w środowisku wirtualnym na stacji takim jak lokalna i automatyczna piaskownica (auto-sandbox).

5. Program antywirusowy musi posiadać możliwość skanowania wybranych plików, folderów/katalogów (również skompresowanych), a także całych dysków (w tym sieciowych) czy partycji.

6. Program antywirusowy musi posiadać możliwość skanowania dowolnego zasobu podłączonego do stacji roboczej np.: dyski zewnętrzne, pamięci USB

7. Program antywirusowy powinien posiadać filtering URL umożliwiający blokowanie konkretnych stron internetowych.

8. Program antywirusowy musi posiadać moduł antywirusowy chroniący w czasie rzeczywistym.

9. Program antywirusowy musi posiadać moduł sprawdzający reputację plików w chmurze.

10. Program antywirusowy musi posiadać dwukierunkowy konfigurowalny z konsoli web firewall z możliwością tworzenia polityk globalnych i z podziałem na aplikacje.

11. Program antywirusowy musi posiadać moduł HIPS (Host Intrusion Protection System – ochrona antywłamaniowa).

12. Program antywirusowy musi posiadać moduł automatycznej piaskownicy (autosandbox), odizolowanego środowiska wirtualnego, w którym zasoby są emulowane dla obiektów w nim umieszczonych. Dodatkowo cały proces izolacji dzięki temu modułowi musi odbywać się lokalnie, na stacji roboczej. Całe środowisko wirtualne musi być odwzorowaniem 1:1 z systemem operacyjnym. Użytkownik powinien móc pracować w zwirtualizowanym środowisku, bez możliwości zapisu na stacji poza środowiskiem wirtualnym.

13. Program antywirusowy musi posiadać możliwość uruchomienia dowolnego pliku/programu w automatycznej piaskownicy (auto-sandbox) na żądanie użytkownika (manualnie).

14. Program antywirusowy musi umożliwiać użytkownikowi wysłanie podejrzanego obiektu do producenta oprogramowania antywirusowego w celu jego analizy. Funkcja ta powinna być dostępna z interfejsu programu antywirusowego.

15. Podczas pracy komputera Program musi automatycznie skanować:
-pliki uruchamiane, otwierane,
-pliki kopiowane lub przenoszone,
-pliki tworzone,
-pliki pobierane z Internetu po protokole HTTP/HTTPS.

16. W przypadku wykrycia wirusa program musi posiadać możliwość automatycznego poddawania kwarantannie podejrzanych obiektów oraz opcję przywrócenia z kwarantanny usuniętych obiektów.

17. Program antywirusowy musi posiadać funkcję dodawania wyjątków do modułu antywirusowego, automatycznej piaskownicy (auto-sandbox) czy modułu HIPS.

18. Program antywirusowy powinien posiadać dodatkowe narzędzie do skanowania systemu.

19. Program antywirusowy musi posiadać dodatkowe narzędzie do analizowania bezpieczeństwa procesów.

20. Program antywirusowy powinien mieć możliwość skanowania skompresowanych plików.

21. Program antywirusowy musi być z możliwością zablokowania dostępu do zmiany ustawień programu hasłem administratora oraz hasłem skonfigurowanym w konsoli zarządzającej.

22. Program antywirusowy powinien mieć możliwość importowania oraz eksportowania ustawień.

23. Program antywirusowy powinien mieć możliwość tworzenia list zaufanych procesów.

24. Program antywirusowy powinien mieć możliwość tworzenia list zaufanych plików.

25. Program antywirusowy i konsola powinny umożliwiać tworzenie wyjątków ze skanowania folderów / plików.

26. Program antywirusowy powinien umożliwiać konfigurację polityk (globalnych ustawień dla grup endpoint'ów) w celu szybkiej implementacji ustawień bezpieczeństwa dla wielu urządzeń.

27. Program antywirusowy powinien umożliwiać zmianę ustawień priorytetu skanowania.

28. Program antywirusowy powinien umożliwiać skanowanie pamięci komputera po uruchomieniu.

29. Program antywirusowy posiada zintegrowaną funkcję skanowania plików pod kątem danych wrażliwych (DLP).

30. Program antywirusowy posiada zintegrowaną funkcję blokowania urządzeń zewnętrznych / przenośnych przed odczytem, edycją i zapisem plików w tym samym czasie.

31. Program antywirusowy posiada zintegrowaną funkcję blokowania jedynie zapisu plików na urządzeniach zewnętrznych / przenośnych.

32. Program antywirusowy powinien posiadać możliwość aktualizowania baz danych antywirusowych ręcznie, nawet jeśli komputer nie będzie miał dostępu do Internetu.

33. Program antywirusowy musi posiadać zintegrowane środowisko, dzięki któremu możemy bezpiecznie działać w wirtualnym systemie nawet na zainfekowanej stacji. Środowisko to musi być odizolowanie od reszty systemu operacyjnego i mieć możliwość uruchomienia takich sesji bez wprowadzonych wcześniejszych zmian przez użytkownika w tym narzędziu (czyste środowisko). Ma również pozwalać na bezpieczniejsze wykonywanie przelewów bankowych, bez obaw, że system operacyjny, na którym działa dany komputer nie został uprzednio zmodyfikowany i byłby w stanie zagrozić utracie np. danych logowania do kont bankowych.

34. Oprogramowanie powinno mieć możliwość przeglądania obciążenia procesów na stacji i serwerze oraz zawartości dysków z poziomu konsoli web.

Dodatkowe systemy bezpieczeństwa

1. Konsola web musi posiadać możliwość śledzenia historii zagrożeń na wybranych komputerach.

2. Konsola web musi posiadać moduł zapobiegania wyciekowi danych DLP z możliwością włączenia skanowania plików w wybranych lokalizacjach na komputerach pod kątem znajdujących się w nich danych wrażliwych przez zdefiniowane wzory z możliwością dodawania własnych reguł DLP oraz powinna umożliwiać sprawdzenia logów z tej czynności.

3. Konsola web zintegrowana z wszystkimi poprzednimi modułami i funkcjami musi umożliwić przeprowadzenia skanowania sieci firmowej (również za pomocą protokołu SNMP) w celu przeprowadzenia audytu urządzeń działających w tej sieci.

Sekcja podsystemu EDR

1. Wbudowany podsystem typu EDR musi rozróżniać i filtrować alerty na min. 10-ciu poziomach (punktowanych) potencjalnego zagrożenia.

2. Wbudowany system EDR musi mieć możliwość tworzenia przez użytkownika własnych polityk bezpieczeństwa w oparciu o instrukcje warunkowe i funkcje logiczne..

3. Wbudowany system EDR musi mieć możliwość śledzenia zdarzeń dotyczących ingerencji w procesy, zmian w rejestrze, operacji na plikach oraz ruchu sieciowego.