**OPIS PRZEDMIOTU ZAMÓWIENIA**

1. system antywirusowy WITH-SECURE Client Security na 500 stanowisk- przedłużenie subskrypcji na 12 miesięcy lub równoważny

System antywirusowy powinien spełniać następujące minimalne lub równoważne parametry:

* Ilość obsługiwanych stanowisk: 500
* Subskrypcja na 12 miesięcy od 30.06.2023 r.
* Interfejs graficzny
* Konsola zarządcza z poziomu przeglądarki lub osobnej aplikacji
* Powiadomienia na e-mail
* Automatyczne aktualizacje wersji klientów z poziomu konsoli zarządczej
* Automatyczne aktualizacje bibliotek
* W przypadku zaproponowania innego systemu Wykonawca zobowiązany jest do wdrożenia systemu u Zamawiającego, przeszkolenia administratorów bez dodatkowych kosztów

Ochrona antywirusowa stacji roboczych musi wspierać następujące systemy operacyjne:

* Microsoft Windows 7 SP1
* Microsoft Windows 8.1
* Microsoft Windows 10
* Microsoft Windows 11

Ochrona antymalware

1. Ochrona musi być realizowana jest na wielu poziomach tj. na poziomie plików, sieci i urządzeń zewnętrznych.
2. Rozwiązanie wyposażone musi być w mechanizmy do wykrywania różnego typu malware, w tym m.in. ransomware, koni trojańskich, robaków, wirusów itp.
3. Rozwiązanie musi być wyposażone w silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu spyware i riskware.
4. Aktualizacje baz definicji wirusów muszą być dostępne 24h na dobę na serwerze producenta - możliwa jest zarówno aktualizacja automatyczna programu oraz na żądanie przez wywołanie funkcji w interfejsie lokalnym oprogramowania.
5. System musi posiadać 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 musi umożliwiać 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 musi posiadać możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
8. Rozwiązanie musi pozwalać na wywołania skanowania po uruchomieniu systemu operacyjnego oraz po zalogowaniu użytkownika.
9. Rozwiązanie musi posiadać możliwość wywołania procesu skanowania z niskim priorytetem, co pozwala na skanowanie z użyciem mniejszej ilości zasobów systemowych.
10. Rozwiązanie musi posiadać możliwość wywołania skanowania wszystkich plików, tylko określnych rozszerzeń plików a także ich wykluczanie.
11. Rozwiązanie musi posiadać możliwość skanowania dysków przenośnych takich jak pendrive, dyski zewnętrzne, czy dyski sieciowe.
12. Rozwiązanie musi pozwalać 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 powinno wykorzystywać 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 powinny posiadać podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
16. Rozwiązanie nie musi wymagać restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
17. Rozwiązanie powinno wykorzystywać w swoim działaniu heurystyczną technologię do wykrywania nowych, nieznanych wirusów.
18. Rozwiązanie powinno pozwalać na wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger”, „dialer”, „trojan”, „rootkit” oraz ataki typu 0-day.
19. Rozwiązanie powinno wykorzystywać mechanizm wykrywania nowych i nieznanych zagrożeń (0-day), analizujący podejrzane pliki wykonywalne.
20. Rozwiązanie musi pozwalać 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 musi pozwalać na integrację z AMSI
22. Ochrona plików w czasie rzeczywistym powinna pozwalać na wykluczenie ze skanowania procesów.
23. Funkcja skanowania dysków sieciowych powinna pozwalać na skanowanie wszystkich plików, do których uzyskiwany jest dostęp lub tylko plików wykonywanych z takich zasobów.
24. Użytkownik ma mieć możliwość uwolnienia pliku poddanego kwarantannie.
25. Uwolnienie pliku z kwarantanny powinno odbywać się po podaniu hasła ustalonego przez administratora.
26. W przypadku wykrycia szkodliwego pliku rozwiązanie musi umożliwiać 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 musi zawierać funkcje logowania historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów możliwy będzie z poziomu GUI aplikacji.
30. Rozwiązanie automatycznie musi powiadamiać użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.
31. Administrator ma mieć możliwość wyłączenia powiadomień dla użytkowników stacji końcowej o wykrytych zagrożeniach.

Ochrona ruchu HTTP

1. Rozwiązanie powinno skanować na komputerze klienckim, dane pobierane i wysyłane przy pomocy protokołu http.
2. Administrator musi posiadać 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 powinno realizować ochronę podczas przeglądania sieci Internet na podstawie badania reputacji witryn.
4. Rozwiązanie musi pozwalać na graficzną informację dotycząca reputacji witryn wyświetlanych w wynikach wyszukiwania za pomocą wyszukiwarek takich jak Google, Bing.

Zapora sieciowa

1. Rozwiązanie musi posiadać 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 powinno posiadać wbudowane predefiniowane profile.
3. Profile bezpieczeństwa zapory ogniowej powinny zawierać predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.
4. Administrator powinien posiadać możliwość określenia domyślnej reakcji dla nieznanej komunikacji sieciowej dla ruchu przychodzącego i wychodzącego.
5. Jako domyślne akcje dla nieznanego ruchu sieciowego rozwiązanie powinno pozwalać określić blokowanie lub zezwolenie na taką komunikację.
6. Administrator musi posiadać możliwość stworzenia reguł stosowanych w przypadku aktywacji izolacji hosta od sieci.

Kontrola nośników zewnętrznych

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

Dodatkowe funkcje

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

**Opis systemu centralnego zarządzania**

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

Instalacja sytemu centralnego zarządzania dla Microsoft Windows musi wspierać 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 musi wspiera następujące 64 bitowe wersje systemów operacyjnych:

* Red Hat Enterprise Linux 6,7,8
* CentOS 7, 8
* SuSE Linux Enterprise Server 11, 12, 15
* SuSE Linux Enterprise Desktop 11, 12, 15
* Debian GNU Linux 9, 10
* 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 ma być zaszyfrowana.
3. Rozwiązanie powinno pozwalać na scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola ma pozwalać na zdalne zarządzanie wszystkimi ustawieniami klienta.
4. Administratorzy mają mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.
5. Centralna konsola administracyjna ma umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy.
6. Rozwiązanie ma pozwalać na tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach.
7. Rozwiązanie ma pozwalać na import struktury drzewa z Microsoft Active Directory.
8. Rozwiązanie ma pozwalać na tworzenie reguł synchronizacji z Microsoft Active Directory umożliwiających automatyczną synchronizację klientów z aktualnie istniejącymi grupami komputerów.
9. Rozwiązanie ma pozwalać na tworzenie reguł powiadamiania o nowych, niezarządzanych klientach w Microsoft Active Directory.
10. Rozwiązanie ma pozwalać na blokowanie wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników.
11. Rozwiązanie ma pozwalać na zdefiniowania hasła do odinstalowania aplikacji.
12. Rozwiązanie ma pozwalać na definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów.
13. Rozwiązanie ma posiadać 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 ma umożliwiać 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 ma pozwalać na konfigurację włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.
16. Rozwiązanie ma umożliwiać administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki.
17. Rozwiązanie ma pozwalać na eksport raportów z pracy systemu do pliku HTML.
18. Rozwiązanie ma dawać możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich.
19. Rozwiązanie ma posiadać 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 ma umożliwiać wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora.
21. Zarządzanie zdarzeniami i raportowanie ma pozwalać 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 ma dawać możliwość przekierowania alertów bezpośrednio do serwera Syslog.
23. Rozwiązanie ma umożliwiać tworzenie wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).
24. Rozwiązanie ma umożliwiać wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączania programu.
25. Wykonywanie automatycznej kopii bazy danych systemu zarządzania centralnego ma odbywać się zgodnie z harmonogramem określonym przez administratora.
26. Administrator ma posiadać możliwość określenia liczby kopii bazy danych, jaka będzie przetrzymywana przez automatyczny system tworzenia kopii zapasowej.
27. Rozwiązanie ma posiadać możliwość wygenerowania danych diagnostycznych z podpiętych komputerów za pomocą konsoli zarządzającej.
28. Rozwiązanie ma posiadać możliwość bezpośredniego pobrania z komputera danych diagnostycznych z poziomu konsoli zarządzającej.
29. Administrator ma posiadać 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 ma pozwalać na tworzenie profili w zależności od systemu operacyjnego i wersji wykorzystywanego w organizacji oprogramowania służącego ochronie.