PYTANIA I ODPOWIEDZI			
Nr pytania	**Referencja do RFI**	**Treść Pytania**	**Odpowiedź EITE**
1.	Dotyczy pkt 1.14. „Możliwość cofnięcia procesu aktualizacji definicji wirusów i mechanizmów skanujących – powrót do poprzedniego zastawu definicji wirusów bez konieczności deinstalacji oprogramowania czy też restartu komputerów”.	Czy Zamawiający dopuści możliwość dostarczenia oprogramowania, które pozwala na cofnięcie procesu aktualizacji, ale wymaga restartu komputera?	TAK, ale restart musi potwierdzic użytkownik
2.	Dotyczy pkt 1.17. „Aktualizacja baz definicji musi być aplikowana tylko w czasie nieaktywności użytkownika na komputerze – jeżeli użytkownik komputera na nim pracuje, aplikacja automatycznie zostaje opóźniona”.	Proces aktualizacji baz definicji jest jednym z najważniejszych elementów, niezbędnych do zapewnienia ciągłej ochrony użytkownika przed zagrożeniami i zawsze powinien być wykonywany tak szybko, jak to możliwe. Czy wobec tego Zamawiający dopuści możliwość dostarczenia produktu, który wymusi aktualizację niezależnie od poziomu utylizacji maszyny, aby skuteczniej ją ochronić?	TAK
3.	Dotyczy pkt 1.21. „Dedykowany moduł analizy w czasie rzeczywistym musi być aktualizowany niezależnie od ochrony antywirusowej poprzez konsolę zarządzającą oraz niezależnie, w postaci pliku exe, który można bezpośrednio uruchomić na kliencie”.	W przypadku nowoczesnych rozwiązań do ochrony anty-wirusowej oraz anty-malware agent zbudowany jest w sposób modularny – wszystkie funkcje ochrony są uruchamiane oraz aktualizowane z konsoli zarządzającej na żądanie administratora. Nie ma możliwości uruchomienia procesu aktualizacji pojedynczego komponentu ochrony w postaci pliku exe bezpośrednio na kliencie. Można natomiast, z poziomu klienta, wymusić proces aktualizacji agenta i jego konfiguracji. Czy wobec tego Zamawiający dopuści możliwość dostarczenia oprogramowania, które umożliwia aktualizację modułów agenta (w tym modułu analizy w czasie rzeczywistym) z poziomu lokalnej konsoli (bezpośrednio na kliencie) oraz centralnie, z systemu zarządzania, nie oferując opcji aktualizacji poprzez uruchomienie pliku exe bezpośrednio na kliencie?	tak

4.	Dotyczy pkt 1.29. „Produkt musi umożliwić utworzenie grup, które będą miały prawo uruchamiać ściągniętą aplikacje, jeżeli będzie z niej korzystać w Internecie zdefiniowana ilość użytkowników (przynajmniej: 5, 50, 100, setki użytkowników) oraz dana aplikacja będzie widziana w Internecie od określonej ilości dni”.	Czy Zamawiający dopuści dostarczenie produktu, który będzie posiadał możliwość tworzenia grup z prawami do uruchomienia ściągniętej aplikacji na podstawie odpowiedniej, definiowanej przez producenta metryki (1-5 gwiazdek), tworzonej w oparciu o globalną ilość użytkowników oraz reputację aplikacji?	tak
5.	Dotyczy pkt 1.32. „Dla systemów typu Windows Embedded wsparcie dla Windows Embedded write filters w tym dla File-Based Write Filter (FBWF)”.	Czy Zamawiający dopuści możliwość dostarczenia oprogramowania bez wsparcia dla FBWF, ale wspierającego systemy Windows Embeded?	tak
6.	Dotyczy pkt 2.7. „Konfiguracja zezwalanego i zabronionego ruchu ma się odbywać w oparciu o takie informacje jak: interfejs sieciowy, protokół, stacja docelowa, aplikacja, godzina komunikacji”.	Czy zamawiający dopuści możliwość dostarczenia oprogramowania, które pozwala na konfigurację zezwalanego i zabronionego ruchu w oparciu o takie informacje jak: interfejs sieciowy, protokół, stacja docelowa, aplikacja oraz lokalizacja agenta, zamiast godziny komunikacji? Dzięki możliwości zdefiniowania reguły na podstawie lokalizacji można skuteczniej dopasować politykę filtrowania ruchu do potrzeb pracy z biura i pracy poza biurem, niezależnie od czasu nawiązania połączenia?	tak
7.	Dotyczy pkt. 2.12. „Uniemożliwianie określenia systemu operacyjnego i rodzaju przeglądarki internetowej przez serwery www”.	Jaką funkcję bezpieczeństwa ma realizować zdefiniowana powyżej funkcja oprogramowania? Czy Zamawiający dopuści możliwość dostarczenia produktu nie posiadającego funkcji uniemożliwiania określenia systemu operacyjnego i rodzaju przeglądarki internetowej przez serwery www? Funkcja tego typu może spowodować nieprawidłowe działanie wielu aplikacji i nie poprawia znacząco poziomu bezpieczeństwa stacji końcowej?	tak

8.	Dotyczy pkt 2.13. „Uniemożliwienie określenia systemu operacyjnego poprzez analizę pakietów sieciowych wysyłanych przez stację”.	Jaką funkcję bezpieczeństwa ma realizować zdefiniowana powyżej funkcja oprogramowania? Czy Zamawiający dopuści możliwość dostarczenia produktu nie posiadającego funkcji uniemożliwienia określenia systemu operacyjnego poprzez analizę pakietów sieciowych wysyłanych przez stację? Funkcja tego typu może spowodować nieprawidłowe działanie wielu aplikacji i nie poprawia znacząco poziomu bezpieczeństwa stacji końcowej?	tak
9.	Dotyczy pkt 3.1. „Producent ma dostarczyć bibliotekę atakówi i podatności (sygnatur) stosowanych przezprodukt. Administrator ma mieć możliwość uaktualniania tej biblioteki poprzez konsolę zarządzającą oraz niezależnie, w postaci pliku exe, który można bezpośrednio uruchomić na kliencie.”	W przypadku nowoczesnych rozwiązań do ochrony anty-wirusowej oraz anty-malware agent zbudowany jest w sposób modularny – wszystkie funkcje ochrony są uruchamiane oraz aktualizowane z konsoli zarządzającej na żądanie administratora. Nie ma możliwości uruchomienia procesu aktualizacji pojedynczego komponentu ochrony w postaci pliku exe bezpośrednio na kliencie. Można natomiast, z poziomu klienta, wymusić proces aktualizacji agenta i jego konfiguracji. Czy wobec tego Zamawiający dopuści możliwość dostarczenia oprogramowania, które umożliwia aktualizację modułów agenta (w tym modułu IPS) z poziomu lokalnej konsoli (bezpośrednio na kliencie) oraz centralnie, z systemu zarządzania, nie oferując natomiast opcji aktualizacji poprzez uruchomienie pliku exe bezpośrednio na kliencie? Producent dostarczy oczywiście bibliotekę ataków i podatności (sygnatur).	tak
10.	Dotyczy pkt. 3.2. „Biblioteka ataków i podatności musi zawierać przynajmniej 4500 sygnatur.”	Czy Zamawiający dopuści produkt, który posiada ponad 2600 sygnatur zgrupowanych w dwóch predefiniowanych zestawach (optymalne ze względu na wydajność, optymalne ze względu na bezpieczeństwo) w celu łatwiejszego wdrożenia ochrony IPS?	tak
11.	Dotyczy pkt 3.3. „Biblioteka sygnatur musi zawierać również sygnatury dotyczące działalności programów P2P.”	Czy Zamawiający dopuści produkt oferujący możliwość ochrony przed programami P2P w module kontroli aplikacji zamiast w module IPS?	tak
12.	Dotyczy Pkt. 3.4. „Produkt ma mieć możliwość tworzenia własnych wzorców włamań (sygnatur), korzystając z semantyki Snort’a. Sygnatury te mogą działać w trybie blokuj lub rejestruj.”	Czy Zamawiający dopuści produkt, którego mechanizm IPS nie umożliwia tworzenia własnych wzorców włamań, lecz korzysta z wzorców dostarczanych przez Producenta (także poza cyklem aktualizacji, w przypadku szybko rozprzestrzeniających się zagrożeń). Sygnatury te mogą działać w trybie blokuj lub rejestruj?	tak

13.	Pkt. 4.14. „Możliwość automatycznego importu list zarówno białej, jaki i czarnej, co zdefiniowany interwał czasu”.	Czy Zamawiający dopuści dostarczenie produktu, który oferuje możliwość importu czarnej listy za pomocą interfejsu programistycznego API w formacie STIX (Structured Threat Information eXpression) z opcją blokowania lub logowania?	tak
14.	Pkt. 8.11. „Możliwość ograniczenia pasma sieciowego od serwera zarządzającego do jego klientów w zależności od ściąganych definicji, aktualizacji klienckiej, podsieci, z której się łączą.”	Czy poprzez ograniczenie pasma sieciowego Zamawiający rozumie możliwość dostarczenia produktu z hierarchiczną strukturą opartą na tzw. agentach aktualizacji, których można umieścić w lokalizacjach lub podsieciach w których jest problem z pasmem sieciowym? Dzięki temu aktualizacje do tych lokalizacji mogą spływać tylko raz, oszczędzając pasmo sieciowe. Pozostałe systemy w danej podsieci pobierają swoje aktualizacje od agenta aktualizacji i nie wymagają pasma sieciowego do serwera zarządzającego.	tak
15.	Dotyczy Pkt 9.5. „inwentaryzacje stacji roboczych (w tym wielkość dysku, zajętość dysku, wielkość pamięci RAM, wykorzystywany system operacyjny oraz procesor)”.	Czy Zamawiający dopuści możliwość dostarczenia produktu, który będzie raportował o: Systemie operacyjnym, procesorze oraz o zalogowanym użytkowniku, a o pamięci i dysku twardym w przypadku wystąpienia problemów z ich dostępnością?	tak
16.	Dotyczy pkt. 9.10 Produkt musi umożliwiać automatyczne zbudowanie zapytań, które będą wykonywane o zdanym czasie i ich wynik będzie przechowywany w postacie kostek OLAP. Powstałe kostki muszą umożliwiać wykonywanie na nich typowych operacji takich jak zwijanie/agregacja danych, rozwijanie (bardziej szczegółowe dane), selekcja (wybór intersujących danych). Wszystkie te operacje muszą być wykonywane graficznie.	Czy Zamawiający mógłby doprecyzować, jakich danych mają dotyczyć zdefiniowane zapytania? Czy dopuszczona może być alternatywna do kostek OLAP forma raportowania?	tak

17.	Dotyczy pkt. 10.14. „lokalizacja ma być określana według istnienia lub nieistnienia: typu interfejsu sieciowego, numeru MAC domyślnej bramki, adresu IP, zakresu podsieci, wartości kluczy w rejestrze, komunikacji z serwerem zarządzającym, nazwy domeny, adresów serwerów WINS, DNS, DHCP, wyniku zapytania do serwera DNS.”	Czy Zamawiający dopuści możliwość dostarczenia produktu, który potrafi ustalić lokalizację agenta na podstawie podłączenia do swojego serwera zarządzającego lub parametrów bramy domyślnej podsieci, w której się znajduje?	tak
18.	Dotyczy pkt. 10.16. „paczki instalacyjne produktu mają pozwalać na dodanie własnej konfiguracji”.	Czy Zamawiający dopuści możliwość dostarczenia produktu, którego konfiguracji dokonuje się za pomocą polityk z centralnego systemu zarządzania, po instalacji agenta z generycznej paczki instalacyjnej? Polityki bezpieczeństwa mogą zostać automatycznie przydzielone na podstawie np. przynależności do grupy w domenie AD lub cech urządzenia końcowego (np. fragmentu jego nazwy, adresu IP itp.).	tak
19.	Dotyczy pkt. 10.20. „Produkt ma automatycznie wykrywać wszystkie urządzenia przyłączone do sieci komputerowej.”	Czy Zamawiający ma na myśli wszystkie stacje końcowe oraz serwery do ochrony, obecne w drzewie usługi katalogowej Active Directory?	tak
20.	Dotyczy pkt. 10.23. „Oficjalna dokumentacja schematu bazy danych, z której korzysta system zarządzający”.	Czy Zamawiający dopuści możliwość dostarczenia produktu, który nie posiada, ze względów bezpieczeństwa, publicznej dokumentacji bazy danych?	tak
21.	Dotyczy pkt. 13.2. Klient dla system Linux ma być zarządzany przez ten sam serwer oraz z tej samej konsoli zarządzającej, co klienci Windows.	Czy Zamawiający dopuści dostarczenie oprogramowania, które do ochrony Linux’a używa dedykowanego systemu zarządzanego z innej konsoli, lecz posiadającego możliwość integracji z systemem dla MS Windows na poziomie logów? Ponadto system ten może zrealizować funkcje ochrony także poprzez mechanizmy reputacji sieciowej, co znacząco zwiększy poziom bezpieczeństwa maszyn z Linux’em.	tak

22.	Dotyczy pkt. 5. Mechanizm pułapek	Opis mechanizmu pułapek wskazuje jednoznacznie na jednego producenta (Symantec) i nie pozwala dostarczyć alternatywnych rozwiązań, ograniczając konkurencję wśród Dostawców. https://docs.broadcom.com/doc/a-look-at-deception-en Rozumiemy, że intencją Zamawiającego było zakupienie systemu AV który pozwala także na ochronę przed nowymi, nieznanym zagrożeniami, w tym przed atakami ukierunkowanymi. Istnieją na rynku inne metody ochrony niż specyficzny dla Symantec'a mechanizm pułapek. W nowoczesnych produktach AV funkcje te są realizowane w ramach komponentu Endpoint Detection and Response (EDR). Dlatego prosimy, aby zamawiający dopuścił możliwość zaoferowania alternatywnego systemu, który będzie mógł być rozbudowany o komponent EDR oraz mechanizmy bazujące na tzw. IoA (indicators of attack) do detekcji nowych, nieznanych zagrożeń zgodnie z macierzą Mitre ATT&CK: https://attack.mitre.org	tak
23.	Dotyczy pkt. 6. Integralności komputera	Opis mechanizmu sprawdzania Integralności Komputera wskazuje jednoznacznie na jednego producenta (Symantec) i nie pozwala dostarczyć alternatywnych rozwiązań, ograniczając konkurencję wśród Dostawców. https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Monitoring-Reporting-and-Enforcing-Compliance/setting-up-host-integrity-v33444962-d57e99/how-host-integrity-works-v85696746-d57e6.html Rozumiemy, że intencją Zamawiającego było zakupienie systemu AV który pozwala także na ochronę przed zaawansowanymi zagrożeniami. W nowoczesnych produktach dostępnych obecnie na rynku funkcje te są realizowane w ramach komponentu Endpoint Detection and Response (EDR). Dlatego prosimy, aby zamawiający dopuścił możliwość zaoferowania alternatywnego systemu, który będzie posiadał możliwość rozbudowy właśnie o element Endpoint Detection and Response realizujący podobne funkcje.	tak
24.	Ogólne	Ponieważ mechanizm szyfrowania mail'i może istnieć jako osobny moduł, a nawet osobny produkt, w którym specjalizują się niektóre firmy i bardzo często nie jest w obszarze zainteresowań Vendor'ów rozwijajacych produkty antywirusowe, zwracamy się z uprzejmą prośbą o wyłączenie tej części z projektu lub utworzenie z niej osobnego zadania, ocenianego niezależnie od części antywirusowej.	Szyfrowanie poczty możemy wyłaczyć z postepowania
25.		Czy zamawiający dopuszcza rozwiązanie, które zamiast centralnej kwarantanny, dostarczy kwarantannę lokalną dla każdej stacji, przy czym zarządzanie będzie centralne - możliwość pobierania wszystkich plików z kwarantanny w jedno centralne miejsce (np. udział sieciowy)?	tak

26.		Czy zamawiający dopuszcza rozwiązanie, które zamiast aplikowania tylko w czasie nieaktwności użytkownika, będzie aplikowało w trakcie pracy, w sposób cichy, niewpływający na pracę uzytkownika?	tak
27.		Czy zamawiający dopuszcza rozwiązanie, które zamiast co najmniej 150 milionów sond, posiada co najmniej 110 milionów sond?	tak
28.	1.21	1.21 Czy zamawiający dopuszcza rozwiązanie, które zamiast aktualizacji modułu analizy ochrony w czasie rzeczywistym w sposób niezależny i w postaci pliku exe, będzie aktualizowało moduł ochrony w czasie rzeczywistym razem z aktualizacją wszystkich modułów ochronnych (w tym sygnatury baz wirusów). Aktualizacja ta będzie możliwa bezpośrednio z serwerów producenta, przy wykorzystaniu proxy (które może być postawione na serwerze wraz z konsolą zarządzającą), z plików offline oraz z repozytorium (kopia dystrybucyjna), tworzonego przez innego klienta.	tak
29.	1.29	1.29 Czy zamawiający dopuszcza rozwiązanie, które zamiast możliwości ustawiania zdefiniowanej ilości użytkowników oraz widoczności aplikacji w sieci Internet od określonej liczby dni, zablokuje automatycznie pliki w przypadku wykrycia zagrożenia oraz małą ilość użytkowników, korzystających z plików i małą reputację.	tak
30.	1.33	1.33 Czy zamawiający dopuszcza rozwiązanie, które zamiast posiadania dwóch wersji sygnatur - pełnej oraz uproszczonej, będzie posiadać jedną pełną wersję sygnatur, która pozwoli w pełni wykrywać wszelkiego rodzaju zagrożenia także w systemach VDI. Same aktualizacje nie będą wpływały znacząco na pobieranie miejsca w systemach VDI.	tak
31.	1.35	1.35 Czy zamawiający dopuszcza rozwiązanie, które zamiast co najmniej 150 milionów sond, posiada co najmniej 110 milionów sond?	tak
32.	2.7	2.7 Czy zamawiający dopuszcza rozwiązanie, które zamiast godziny komunikacji, pozwoli na zbudowanie reguły w oparciu o zakres portów zdalnych i lokalnych oraz w oparciu o usługę, wykorzystywaną lokalnie?	tak
33.	2.8	2.8 Czy zamawiający dopuszcza rozwiązanie, które zamiast konfiguracji stacji, pozwoli na zrealizowanie reguł firewall w oparciu kierunek, czynność, protokół, profil sieci (w tym połączenie sieciowe - Wifi, Ethernet), lokalne zakresy adresów IP, lokalne zakresy portów, zdalne zakresy portów, zdalne zakresy adresów IP	tak
34.	2.9	2.9 Czy zamawiający dopuszcza rozwiązanie, które jako nagrywanie, dopuszcza zapisywanie informacji o wszytskich połączeniach w dzienniku programu	tak
35.	2.10	2.10 Czy zamawiający dopuszcza rozwiązanie, które zamiast dodawania własnego komunikatu, wyświetli komunikat w języku, w jakim zostanie zainstaloiwany klient - brak ograniczenia licencyjnego do instalowanej wersji językowej. Klient występuje w językach polskim, angielskim i w innych.	tak
36.	2.11	2.11 Czy zamawiający dopuszcza rozwiązanie, które zamiast wysyłania wiadomości do administratora, prześle wszystkie logi do serwera zdalnej administracji, które następnie wyświetli jako raport.	tak

37.	1	.1 Czy zamawiający dopuszcza rozwiązanie, które zamiast aktualizacji modułu analizy ochrony przed włamaniami IPS w sposób niezależny i w postaci pliku exe, będzie aktualizowało moduł ochrony przed włamaniami razem z aktualizacją wszystkich modułów ochronnych (w tym sygnatury baz wirusów). Aktualizacja ta będzie możliwa bezpośrednio z serwerów producenta, przy wykorzystaniu proxy (które może być postawione na serwerze wraz z konsolą zarządzającą), z plików offline oraz z repozytorium (kopia dystrybucyjna), tworzonego przez innego klienta.	tak
38.	3.2	3.2 Czy zamawiający dopuszcza rozwiązanie, które zamiast posiadania 4500 sygnatur, będzie posiadać sygnatury, które będą chronić przed wszelkiego rodzaju anomaliami w sieci	tak
39.	3.3	3.3 Czy zamawiający dopuszcza rozwiązanie, które zamiast sygnatur P2P, będzie posiadało kontrolę dostępu do stron internetowych, pozwalającą na blokowanie stron z kategorii P2P	tak
40.	3.4	3.4 Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało funkcjonalności tworzenia własnych wzorców włamań	tak
41.	3.10	3.10 Czy zamawiający dopuszcza rozwiązanie, które zamiast określania zdefiniowanego czasu, pozwoli administratorowi na zablokowanie ruchu ze stacjami uznanymi za wrogie do momentu odblokowania tego ruchu rzed administratora.	tak
42.	3.12	3.12 Czy zamawiający dopuszcza rozwiązanie, które zamiast wymienionych technik ochrony oraz języków Java i VLC, chroni przed wykorzystaniem luk w programach firm trzecich, typu system operacyjny, java, przeglądarki webowe oraz czytniki PDF	tak
43.	4.4	4.4 Czy zamawiający dopuszcza rozwiązanie, które będzie rozpoznawało aplikacje po nazwie i po ścieżce?	tak
44.	4.7	4.7 Czy zamawiający dopuszcza rozwiązanie, które zamiast logowania plików, wgrywanych na urządzenie, będzie blokowało nośniki zewnętrzne, by pliki nie wyciekły i dopuszczały tylko autoryzowane nośniki, przekazane przez administratorów	tak
45.	4.11	4.11 Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało funkcjonalności białej listy zaufanych aplikacji?	nie
46.	4.14	4.14 Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało funkcjonalności białej listy zaufanych aplikacji?	nie
47.	5	5. Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało funkcjonalności mechanizmu pułapek?	tak
48.	6.4	6.4 Czy zamawiający dopuszcza rozwiązanie, które zamiast tworzenia niestandardowego testu integralności, automatycznie będzie pokazywać wszystkie niespełnione warunki jako alert w konsoli zdalnego zarządzania, bez konieczności stosowania składni If...Then...Else	tak
49.	7.2	7.2 Czy zamawiający dopuszcza rozwiązanie, które zamiast wykluczania wszystkich plików ze złotego obrazu, przeskanuje każdy element tylko raz i jeśli w przyszłości nie zostanie zmodyfikowany to taki element nie będzie powtórnie skanowany w celu ograniczenia wykorzystania zasobów?	tak

50.	7.3	7.3 Czy zamawiający dopuszcza rozwiązanie, które zamiast współdzielenia wyników skanowania tego samego pliku, pozwoli na przeskanowanie	tak
51.	7.6	7.6 Czy zamawiający dopuszcza rozwiązanie, które zamiast posiadania dwóch wersji sygnatur - pełnej oraz uproszczonej, będzie posiadać jedną pełną wersję sygnatur, która pozwoli w pełni wykrywać wszelkiego rodzaju zagrożenia także w systemach VDI. Same aktualizacje nie będą wpływały znacząco na pobieranie miejsca w systemach VDI.	tak
52.	8.6	8.6 Czy zamawiający dopuszcza rozwiązanie, które zamiast replikacji informacji między serwerami, pozwoli drugiemu serwerowi na przeniesienie bazy danych ze wszystimi informacjami i podpięcie jej do drugiego serwera, tak by wszystkie zapisane informacje były dostępne na drugim serwerze	tak
53.	8.7	8.7 Czy zamawiający dopuszcza rozwiązanie, które zamiast określenia zajętości na dysku oraz konfiguracji prędkości, pozwoli na wystawienie wstępnych aktualizacji, regularnych i opóźnionych aktualizacji, by nie doszło do false-positive?	tak
54.	8.10	8.10 Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało funkcjonalności dedykowanego narzedzia służącego do monitorowania klientów, którzy zostali dostarczycielami aktualizacji?	tak
55.	8.11	8.11 Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało funkcjonalności ograniczenia pasma?	nie
56.	9.10	9.10 Czy zamawiający dopuszcza rozwiązanie, które zamiast budowania kostek OLAP, pozwoli na korzystanie z ponad 170 gotowych szablonów stworzonych przez producenta. Szablony raportów moga być edytowane i moga być tworzone nowe od zera. Szablony pozwalają na wykorzystanie ponad 1000 elementów, które są przekazywane przez agenta ze stacji do serwera zdalnej administracji.	tak
57.	9.11	9.11 Czy zamawiający dopuszcza rozwiązanie, które zamiast budowania trendów, pozwoli na wyświetlanie raportów po przefiltrowaniu do zakresów dat, by zweryfikować zachowanie użytkowników, działanie systemów operacyjnych i uruchomionych aplikacji/zagrożeń, itp.	tak
58.	10.14	10.14 Czy zamawiający dopuszcza rozwiązanie, które zamiast określenia lokalizacji za pomocą numeru MAC bramki, wartości kluczy w rejestrze, wyniku zapytania do serwera DNS pozwoli na określenie lokalizacji za pomocą adresu IP bramy, przyrostka DNS, identyfikatora bezprzewodowego SSID, nazwy sieci bezprzewodowej, typu zabezpieczeń sieci bezprzewodowej i typu szyfrowania?	tak
59.	10.15	10.15 Czy zamawiający dopuszcza rozwiązanie, które będzie miało tylko możliwość stosowania operatora logicznego "I" dla wszystkich wcześniej wspomnianych elementów, a dla części z nich możliwy będzie operator logiczny "LUB"	tak
60.	10.19	10.19 Czy zamawiający dopuszcza rozwiązanie, które będzie automatycznie dystrybuować nowe wersje po wcześniejszym wybraniu zadania i utworzenia grupy dynamicznej dla takiej nowszej wersji?	tak

61.	10.22	10.22 Czy zamawiający dopuszcza rozwiązanie, które zamiast określenia pasma dla klientów, pozwoli na ograniczanie pasma dla przesyłania informacji pomiędzy agentem, a serwerem?	tak
62.	10.23	10.23 Czy zamawiający dopuszcza rozwiązanie, które zamiast dokumentacji bazy danych, nie wymaga od administratora żadnych czynności związanych z edycją w bazie danych, a całość zarządzania dostepne jest z poziomu konsoli zdalnego zarządzania, bez dostawania się do bazy danych	tak
63.	11.1.2	11.1.2 Czy Zamawiający dopuszcza dostarczenie przedmiotu zamówienia bez wsparcia agenta i klienta antywirusowego dla systemu Vista, w związku z faktem, że dostawca systemu operacyjnego Vista, firma Microsoft, nie dostarcza wsparcia i poprawek bezpieczeństwa dla niego i nie jest w związku z tym możliwe pełne zabezpieczenie tego systemu?	tak
64.	11.3.1	11.3.1 Czy Zamawiający dopuszcza dostarczenie przedmiotu zamówienia bez wsparcia serwera zarządzania dla systemu Windows 2008, w związku z faktem, że dostawca systemu operacyjnego Windows 2008, firma Microsoft, nie dostarcza wsparcia i poprawek bezpieczeństwa dla niego i nie jest w związku z tym możliwe pełne wsparcie tego systemu?	nie
65.	11.3.2	11.3.2 Czy Zamawiający dopuszcza dostarczenie przedmiotu zamówienia bez wsparcia serwera zarządzania dla systemu Windows 2008 R2, w związku z faktem, że dostawca systemu operacyjnego Windows 2008 R2, firma Microsoft, nie dostarcza wsparcia i poprawek bezpieczeństwa dla niego i nie jest w związku z tym możliwe pełne wsparcie tego systemu?	nie
66.	13.1	13.1 Czy zamawiający dopuszcza rozwiązanie, które będzie wspierało w pełni Ubuntu Desktop 18.04 LTS 64-bit, Red Hat Enterprise Linux 7, RedHat Enterprise Linux (RHEL) 6 64-bit, RedHat Enterprise Linux (RHEL) 7 64-bit, CentOS 6 64-bit, CentOS 7 64-bit, Ubuntu Server 16.04 LTS 64-bit, Ubuntu Server 18.04 LTS 64-bit, Debian 9 64-bit, SUSE Linux Enterprise Server (SLES) 12 64-bit, SUSE Linux Enterprise Server (SLES) 15 64-bit. Wymogiem koniecznym będzie brak konieczności kompilowania oprogramowania dla tych platform systemowych.	tak
67.	1.2	1.2 Czy zamawiający dopuszcza rozwiązanie, które nie będzie współpracowało z centrum certyfikacji, tylko będzie posiadało własne klucze?	nie
68.	2.5	2.5 Czy Zamawiający dopuszcza dostarczenie przedmiotu zamówienia bez wsparcia rozwiązania do szyfrowania dla systemów XP, Vista, w związku z faktem, że dostawca systemów operacyjnych XP,Vista, firma Microsoft, nie dostarcza wsparcia i poprawek bezpieczeństwa dla nich i nie jest w związku z tym możliwe pełne zabezpieczenie tego systemu?	tak
69.	2.13	2.13 Czy zamawiający dopuszcza rozwiązanie, które zamiast ukrywania ikony, pozwala na wyłączenie funkcjonalności dla klienta, tak by miał tylko dostęp do ważnych elementów systemu (m.in. pomoc i aktualizacja programu)	tak

70.	2.15	2.15 Czy zamawiający dopuszcza rozwiązanie, które zamiast stosowania sprzętowego szyfrowania OPAL, pozwoli na zaszyfrowanie takiego dysku?	tak
71.	2.16	2.16 Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało takiej funkcjonalności	nie
72.	2.17	2.17 Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało takiej funkcjonalności	nie
73.	2.18	2.18 Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało takiej funkcjonalności	nie
74.	2.19	2.19 Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało takiej funkcjonalności	tak
75.	3.4	3.4 Czy zamawiający dopuszcza rozwiązanie, które zamiast deszyfrowania przy użyciu pre-boot, będzie dawało możliwość administratorowi wygenerowanie nośnika, który umożliwi odszyfrowanie stacji	tak
76.	3.9	3.9 Czy zamawiający dopuszcza rozwiązanie, które zamiast formy szyfrowania plików kopiowanych na te urządzenia, będzie szyfrowało całą powierzchnię dysku lub tylko kontener, do którego będzie aplikacja, umożliwiająca dostanie się ze stacji, które nie mają zainstalowanego oprogramowania?	nie
77.	3.12	3.12 Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało takiej funkcjonalności	nie
78.	4.1	4.1 Czy zamawiający dopuszcza rozwiązanie, które zamiast będzie posiadało algorytmy do tworzenia kluczy do wybory: AES 128 bit, 3DES, Blowfish	nie
79.	4.4	4.4 Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało takiej funkcjonalności podpisywania	nie
80.	4.5	4.5 Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało takiej funkcjonalności podpisywania	nie
81.	4.6	4.6 Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało takiej funkcjonalności	nie
82.	4.9	4.9 Czy zamawiający dopuszcza rozwiązanie, które nie będzie posiadało takiej funkcjonalności dla systemu Android, a zamiast będzie posiadało tylko dla iOS?	nie