SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa oraz wdrożenie systemu zarządzania i ochrony urządzeń mobilnych MDM (Mobile Device Management), wraz z kompletem niezbędnych licencji, przeszkoleniem pracowników oraz zapewnieniem wsparcia technicznego dla zaoferowanego systemu.

SŁOWNIK POJĘĆ

Polityka – inaczej zasada MDM to pakiet stanowiący zbiór reguł, które zawierają określone warunki, akcje i/lub wyjątki, możliwe do skonfigurowania przez administratora.

Konsola zarządzająca / web panel - zabezpieczone narzędzie posiadające własne GUI, będące częścią całego systemu MDM, umożliwiające administrację, zarządzanie i monitorowanie. Dostęp do tego narzędzia określony jest rolami posiadającymi odpowiedni zakres uprawnień, najlepiej z poziomu przeglądarki webowej (protokół HTTPS).

Błąd krytyczny - nieprawidłowe działanie systemu MDM powodujące albo całkowity brak możliwości korzystania z oprogramowania, albo takie ograniczenie możliwości korzystania z niego, że przestaje ono spełniać swoje podstawowe funkcje. Przykładem Błędu Krytycznego jest niemożność uruchomienia oprogramowania, brak odczytu/zapisu z bazy danych, utrata danych lub ich spójności, brak możliwości zalogowania użytkownika, niedostępność krytycznych funkcji systemu MDM.

1. W ramach realizacji przedmiotu zamówienia mieści się:

1.1 Dostawa niezbędnych licencji i oprogramowania oferowanego systemu MDM dla 520 urządzeń w ramach zamówienia podstawowego w wersji on premise na okres 24 miesięcy, instalowanej na serwerach zamawiającego;

1.2 Wdrożenie oprogramowania MDM na serwerze Zamawiającego;

1.3 Zamawiający zastrzega sobie możliwość zakupu w ramach prawa opcji licencji dla 80 urządzeń, w razie zaistnienia potrzeby, w terminie obowiązywania umowy. Prawo Opcji może zostać zrealizowane przez Zamawiającego w ramach jednego bądź większej liczby zamówień;

1.4 Świadczenie serwisu i wsparcia technicznego Wykonawcy przez okres obowiązywania umowy licząc od daty podpisania bez uwag protokołu odbioru;

1.5 Przeprowadzenie szkolenia z zakresu administracji zamawianego oprogramowania, dla min. 2 osób z pełnego zakresu zarządzania i administracji zamawianym

oprogramowaniem, zrealizowane najpóźniej w terminie 90 dni kalendarzowych od dnia podpisania protokołu odbioru;

1.6 Przeprowadzenie szkolenia z zamawianego oprogramowania, dla min.10 osób z zakresu wdrażania oprogramowania na urządzeniach mobilnych zamawiającego, zarządzania listą urządzeń mobilnych objętych oprogramowaniem MDM, działania i oferowanych funkcjonalności zamawianego oprogramowania, korzystania ze zdalnej pomocy oraz rozwiązywania problemów technicznych;

1.7 Zapewnienie dostępu do konta wsparcia oprogramowania, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta.

2. Wymagania dotyczące dostawy oprogramowania, wdrożenia oraz licencji:

2.1 System MDM musi być dostarczany w postaci pliku .iso, ova;

2.2 Dostawca zobowiązuje się do instalacji, konfiguracji i wdrożenia oferowanego systemu MDM na serwerze Zamawiającego umożliwiając stabilną pracę oprogramowania MDM,

2.3 Zamawiane oprogramowanie musi być kompatybilne z posiadanym przez Zamawiającego VMware ESXi w wersji 6.7;

2.4 Dostawa musi zostać zrealizowana zgodnie z terminem wskazanym w ofercie Wykonawcy, ale nie później niż 10 dni roboczych od dnia podpisania umowy;

2.5 Wykonawca zobowiązuje się dostarczyć wymagane oprogramowanie oraz licencje pochodzące z legalnego źródła, zakupione w autoryzowanym kanale sprzedaży producenta i objęte standardowym pakietem usług gwarancyjnych świadczonych przez sieć serwisową producenta na terenie Polski;

2.6 Dostawa oprogramowania, aplikacji, modułów, wymaganych do prawidłowego funkcjonowania zaoferowanego systemu MDM, zgodnie z wymaganymi funkcjonalnościami oraz specyfikacją Zamawiającego;

2.7 Dostawa wszystkich licencji wymaganych do poprawnej pracy systemu MDM, zgodnie z wymaganymi funkcjonalnościami opisanymi w specyfikacji (w tym do serwera bazy danych oprogramowania MDM);

2.8 Dostarczone do Zamawiającego licencje muszą być w postaci wygenerowanych na stronie producenta plików licencyjnych lub w formie wygenerowanych i przesłanych emailem przez Wykonawcę plików;

2.9 System musi wspierać wszystkie platformy obecnie dostępne na rynku: iOS (co najmniej od wersji 10.3), iPadOS, Android (co najmniej od wersji 6.0), MacOS, Windows;

3. Wymagania dot. systemu MDM

Oprogramowanie musi umożliwiać:

3.1. Obsługę interfejsu co najmniej w językach: polski i angielski;

3.2. Kontrolę nad urządzeniem przenośnym oraz zdalne zablokowanie i wyczyszczenie urządzenia ze wszystkich danych w razie potrzeby;

3.3. Zdalny podgląd statusu urządzenia oraz sprawdzenie jego lokalizacji i połączonej sieci Wi-fi (uwzględniając adres IP oraz MAC) poprzez natychmiastowe wymuszenie lub zgodnie z interwałem czasowym;

3.4. Grupowanie urządzeń;

3.5. Automatyczne pobieranie, kolekcjonowanie następujących danych eksploatacyjnych urządzeń przenośnych:

3.5.1. Numer wersji oprogramowania OS urządzenia;

3.5.2. Aktualna lista zainstalowanych aplikacji z uwzględnieniem wersji na urządzeniu przenośnym lub grupie urządzeń;

3.5.3. Wyświetlanie listy zainstalowanych profilów / aktualnych polityk na urządzeniu przenośnym lub grupie urządzeń;

3.5.4. Aktualne informacje na temat zajętości pamięci (wbudowanej, kart pamięci) oraz stanu baterii urządzenia przenośnego;

3.5.5. Informacje dotyczące przeprowadzanych napraw i usług serwisowych urządzeń (do wprowadzenia przez operatora w systemie);

3.6. Pełną separację danych prywatnych od danych służbowych np. profil służbowy;

3.7. Integrację MDM z usługą katalogową LDAP (Active Directory) w zakresie pobierania użytkowników i grup do systemu MDM;

3.8. Obsługę pakietu danych Exchange ActiveSync (EAS) na urządzeniach Apple;

3.9. Dostęp do Systemu MDM z wykorzystaniem połączenia SSL poprzez przeglądarkę internetową (protokół HTTPS). Zakres dostępu w celu administrowania musi być określony przez możliwe do skonfigurowania role / konta (np. administrator, helpdesk, operator);

3.10. Edycję widoku w konsoli zarządzającej, w szczególności kontrolę nad danymi jakie są wyświetlane np. model urządzenia, aktualny OS oraz w jaki sposób są posortowane. Widok musi mieć możliwość zapisania (np. poprzez dodanie do „ulubionych”;

3.11. Zarządzanie urządzeniami mobilnymi i wprowadzanie polityk bezpieczeństwa poprzez konsolę zarządzającą;

3.12. Dodawanie urządzeń ręcznie do listy zarządzanych przez MDM na różne sposoby: Dodawanie skanując QR kod, używając modułu NFC, za pomocą edytowalnego linku wysyłanego poprzez SMS z konsoli zarządzającej (integracja z zewnętrzną bramką SMS);

3.13. Wdrożenie urządzeń metodami:
    3.13.1. Google zero touch
    3.13.2. Apple Business Manager/Device Enrollment Program
    3.13.3. Samsung Knox Mobile Enrollment
    3.13.4. Właściciel urządzenia (Android Enterprise Device Owner) / Profil Praca (Android Enterprise Work Profile);
3.14. Wsparcie dla przeglądarek Microsoft Edge, Google Chrome, Mozilla Firefox;
3.15. Wykonanie kopii zapasowej danych na pojedynczym urządzeniu, na wszystkich zarejestrowanych w systemie urządzeniach lub na grupach urządzeń z poziomu konsoli zarządzającej;
3.16. Integrację z systemem typu SIEM (Splunk) w zakresie przekazywania zdarzeń występujących w systemie MDM, komunikując się co najmniej za pomocą syslog;
3.17. Odświeżenie informacji o kartach eSIM dla urządzeń co najmniej z systemem iOS, iPadOS;
3.18. Zarządzanie plikami na urządzeniu mobilnym przynajmniej dla platformy Android;
3.19. Działanie w środowisku w pełni zamkniętym (bez dostępu do sieci internet, w szczególności do usługodawców typu Google, Amazon itp);

4. Monitoring i Blokowanie

Oprogramowanie musi:

4.1. Pozwalać na obsługę szerokiej gamy polityk jak:
    4.1.1. Blokada interfejsu Wi-Fi;
    4.1.2. Blokada interfejsu bluetooth;
    4.1.3. Blokada danych pakietowych;
    4.1.4. Blokada danych pakietowych w roamingu;
    4.1.5. Blokada udostępniania interfejsu przez WiFi, USB;
    4.1.6. Blokada VPN przez sieć komórkową;
    4.1.7. Blokada GPS;
    4.1.8. Włącznie i podtrzymanie działania lokalizacji;
    4.1.9. Blokada Aparatu;
    4.1.10. Blokada opcji programisty;
    4.1.11. Blokada nieznanych źródeł;
    4.1.12. Blokada debugowania USB;
    4.1.13. Blokada nagrywania głosu w aplikacjach;
    4.1.14. Blokada NFC;
    4.1.15. Blokada karty pamięci;
    4.1.16. Blokada trybu samolotowego;

4.1.17. Blokada trybu awaryjnego;
4.1.18. Blokada instalacji aplikacji;
4.1.19. Blokada ustawień telefonu;
4.1.20. Blokada przeglądarki www;
4.1.21. Blokada tworzenia konta email;

4.2. Posiadać możliwość obsługi platformy MacOS w zakresie:
4.2.1. Wyłączenia usług iCloud (Mail, Calendar, Reminder, Address Book, Notes,)
4.2.2. Wyłączenia udostępniania plików przez iTunes
4.2.3. Wyłączenia parowania z Apple TV
4.2.4. Blokadę wykorzystania danych lokalizacyjnych przez wyszukiwarkę

4.3. Pozwalać na monitoring takich danych jak:
4.3.1. Użycie danych pakietowych
4.3.2. Treść SMS
4.3.3. Użycie aplikacji
4.3.4. Rozmowy głosowe

4.4. Automatycznie pobierać i kolekcjonować następujące dane identyfikacyjne urządzeń przenośnych:
4.4.1. Nazwa urządzenia;
4.4.2. Model urządzenia;
4.4.3. Producent urządzenia;
4.4.4. Numer seryjny urządzenia;
4.4.5. Numery ID (co najmniej): numer Telefonu, IMEI, IMSI (ICCID) numer wydrukowany na karcie SIM;

5. Zarządzanie aplikacjami

Zamawiane oprogramowanie musi:

5.1. Pozwalać na blokowanie zainstalowanych oraz niezainstalowanych aplikacji;
5.2. Pozwalać na zabezpieczenie aplikacji hasłem;
5.3. Mieć możliwość zarządzania aktualizacjami OTA;
5.4. Pozwalać na tworzenie białych i czarnych list aplikacji;
5.5. Musi pozwolić na zdalną instalację aplikacji własnych oraz z oficjalnych sklepów dostępnych na urządzeniach;
5.6. Udostępniać możliwość blokowania odinstalowywania przez użytkownika;
5.7. Umożliwiać tworzenie sklepu firmowego (Android);
5.8. Pozwalać na obsługę konfiguracji typu kiosk;
5.9. Umożliwiać konfigurację własnego pulpitu na urządzeniach końcowych;
5.10. Pozwalać na wymuszenie ustawienia blokady ekranu, w zakresie:

5.10.1. Wymuszenie rodzaju blokady
5.10.2. Wymuszenie ilości minimalnych znaków
5.10.3. Ustawienie historii haseł
5.10.4. Wymuszenie złożoności hasła

5.11. Pozwalać na zdalną konfigurację poczty Exchange na urządzeniach końcowych;
5.12. Obsługiwać konteneryzację;
5.13. Posiadać możliwość zarządzania dostępem aplikacji w kontenerze;
5.14. Posiadać możliwość zarządzania urządzeniem w całości z podziałem na strefę konteneryzowaną (COPE);
5.15. Umożliwiać konfigurację aplikacji obsługujących Zarządzane Konfiguracje Google (Google Managed Configuration) dla urządzeń z systemem Android bez pośrednictwa serwerów Google;

6. Zapewnienie Bezpieczeństwa

Zamawiane oprogramowanie musi zapewniać:

6.1. Możliwość konfiguracji polityk dotyczących haseł na urządzeniach mobilnych. Z poziomu systemu MDM musi istnieć możliwość zdefiniowania wymogu zabezpieczenia urządzenia mobilnego przy użyciu hasła lub PIN-u oraz poziomu ich skomplikowania;
6.2. Kolekcjonowanie, przechowywanie oraz odczyt logów, które będą zawierać informacje o wykonanych czynnościach administratorów systemu MDM;
6.3. Możliwość integracji MDM z rozwiązaniem Samsung KNOX co najmniej w wersji 2.0 i nowszych;
6.4. Możliwość zdefiniowania czasu bezczynności, po którym nastąpi automatyczna blokada urządzenia mobilnego;
6.5. Możliwość zdefiniowania maksymalnej ilości prób wpisania hasła, po których nastąpi blokada urządzenia mobilnego – możliwa do zdjęcia jedynie przez administratora systemu MDM;
6.6. Możliwość zdalnego usunięcia danych z urządzenia w przypadku jego zgubienia;
6.7. Możliwość zdalnego zablokowania urządzenia mobilnego;
6.8. Możliwość zablokowania opcji formatowania fabrycznego (FRP) na urządzeniu mobilnym;
6.9. Możliwość wykonania zdalnego resetu urządzenia mobilnego;
6.10. Możliwość automatycznego wyczyszczenia urządzenia w przypadku wykrycia zdefiniowanego przez administratora zagrożenia (np. wymiana karty SIM, brak łączności z systemem MDM przez określony czas);

6.11. Możliwość zdalnego przejęcia kontroli nad ekranem oraz klawiaturą urządzenia mobilnego (po wyrażeniu zgody przez użytkownika);
6.12. Możliwość zablokowania opcji deinstalacji systemu MDM z urządzenia mobilnego z poziomu użytkownika;
6.13. Możliwość zablokowania opcji edycji profilu służbowego urządzenia mobilnego z poziomu użytkownika;
6.14. Wbudowany serwer CA w celu pełnego zarządzania certyfikatami na urządzeniach mobilnych lub umożliwiać integrację z zewnętrznym serwerem CA;
6.15. Integrację z Public Key Infrastructure w celu pełnego zarządzania certyfikatami na urządzeniach mobilnych;
6.16. Logowanie do konsoli www z autoryzacją opartą o protokół SAML;
6.17. Możliwość ustawienia powiadomień na zablokowanym ekranie;
6.18. Możliwość ograniczenia funkcjonalności urządzenia bazując na położeniu geograficznym;
6.19. Możliwość obsługiwania mechanizmów proxy.
6.20. Możliwość informowania administratora o sytuacjach awaryjnych takich jak:
    6.20.1. Zmiana karty SIM,
    6.20.2. Zrootowanie urządzenia,
    6.20.3. Brak kontaktu z urządzeniem przez określony czas.

7. Raportowanie i analityka

Zamawiane oprogramowanie musi zapewniać:

7.1. Możliwość generowania raportów o zarządzanych urządzeniach mobilnych. Raporty muszą zawierać minimum: imię i nazwisko użytkownika, typ i model urządzenia, wersję systemu operacyjnego zainstalowanego na urządzeniu, listę zainstalowanych aplikacji wraz z ich wersją, ilość zajętej i wolnej pamięci, numer seryjny karty SIM, numer IMEI, nr seryjny urządzenia;
7.2. Możliwość uzyskania raportów w czytelnych formatach, takich jak PDF lub formatach do dalszego użytku, np. CSV, TXT lub XLS;
7.3. Możliwość, generowania raportów w oparciu o wskazane urządzenia mobilne, użytkowników bądź grupy w określonym przedziale czasu;
7.4. Automatyczne generowanie raportów (zgodnie z harmonogramem), wysyłanych za pośrednictwem poczty mailowej;
7.5. Generowanie i zarządzanie alertami dotyczącymi urządzeń objętych monitoringiem;
7.6. Zewnętrzne API umożliwiające łączność poprzez HTTPS;

8. Zakres wsparcia technicznego i serwisu dla zakupionego oprogramowania:

8.1. Zakres wsparcia producenta, w terminie obowiązywania umowy, obejmuje:

8.1.1. Dostęp do pomocy technicznej w dni robocze w godzinach 8.00-16.00, przez okres trwania umowy;

8.1.2. Możliwość tworzenia zgłoszeń do pomocy technicznej poprzez wysłanie wiadomości mailowej;

8.1.3. Usługę konsultacji w zakresie konfiguracji, optymalizacji i innych czynności dotyczących zamawianego oprogramowania w ilości 80 roboczogodzin (ang. man-day), zgodnie z zapotrzebowaniem Zamawiającego, możliwych do wykorzystania w terminie obowiązywania umowy. Przy czym Zamawiający zastrzega sobie możliwość wykorzystania minimum 30 roboczogodzin.

8.1.4. Usuwanie usterek i błędów (zwanych Wadami) z zachowaniem poniższych zasad:

a) Usunięcie błędu krytycznego lub wykonanie obejścia błędu krytycznego (umożliwiającego korzystanie z Systemu MDM) nastąpi w czasie 48h od przekazania zgłoszenia przez Zamawiającego. Jeżeli jednak bezpośrednią przyczyną powstania błędu krytycznego Systemu MDM jest wada w oprogramowaniu, usunięcie błędu krytycznego nastąpi poprzez współpracę Wykonawcy z producentem Rozwiązania w terminie możliwie najszybszym z punktu widzenia producenta, nie dłuższym niż 10 dni roboczych od przyjęcia zgłoszenia.

b) Usunięcie innych błędów nastąpi w ciągu 5 dni roboczych od przekazania zgłoszenia przez Zamawiającego.

c) Usunięcie usterek nastąpi w ciągu 10 dni roboczych od przekazania zgłoszenia przez Zamawiającego.

d) W przypadku braku możliwości usunięcia Wad w podanych wyżej terminach, Wykonawca dostarczy i wdroży równoważne rozwiązanie zastępcze (workaround), każdorazowo w terminie usunięcia danej Wady. Rozwiązanie zastępcze musi zostać każdorazowo uzgodnione i zaakceptowane przez Zamawiającego.

e) Rozwiązanie zastępcze może funkcjonować nie dłużej niż 30 dni od daty jego wdrożenia.

8.1.5. Dostęp do poprawek i nowych wersji oprogramowania i/lub systemu;

8.1.6. Dostęp do dokumentacji technicznej, dostępnej co najmniej w języku angielskim;

8.1.7. Dostęp do konta wsparcia oprogramowania, zawierającego dostęp do bazy wiedzy oraz systemu zgłoszeń producenta.