Załącznik do Zapytania o wycenę szacunkową

Szczegółowy opis przedmiotu zamówienia

Przedmiotem zamówienia jest:

1) dostawa subskrypcji oprogramowania Microsoft Enterprise Mobility + Security E3 (EMS E3) lub oprogramowania równoważnego dla 750 użytkowników na okres 25 miesięcy (dalej jako: „Oprogramowanie");
2) wykonanie przez Wykonawcę usługi wdrożenia funkcjonalności zarządzania urządzeniami mobilnymi (MDM);
3) zapewnienie przeprowadzenia certyfikowanych szkoleń z oprogramowania Microsoft Enterprise Mobility + Security E3 (EMS E3) lub oprogramowania równoważnego dla administratorów Zamawiającego;
4) świadczenie usługi wsparcia technicznego przez Wykonawcę.

Celem zamówienia jest zwiększenie bezpieczeństwa funkcjonowania posiadanej przez Zamawiającego usługi Microsoft Office 365 E5 oraz urządzeń końcowych Zamawiającego.

1. Wymagania ogólne:

1) Oprogramowanie musi pochodzić bezpośrednio od producenta lub z oficjalnych i autoryzowanych przez producenta kanałów dystrybucyjnych. Zamawiający wymaga, aby Wykonawca posiadał kwalifikacje i uprawnienia wymagane do prawidłowej realizacji przedmiotu zamówienia;
2) dostęp do portalu producenta w celu dostępu oraz zarządzania licencjami;
3) gwarancja dostępności najnowszej wersji Oprogramowania oraz bieżące jego poprawki i uaktualnienia w trakcie trwania umowy;
4) możliwość wykorzystania wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania, monitorowania i wsparcia technicznego;
5) Zamawiający dopuszcza oferowanie produktów o szerszej niż opisana funkcjonalności.

2. Usługa wdrożenia funkcjonalności zarządzania urządzeniami mobilnymi (MDM):

Wykonawca w terminie do 10 dni roboczych od dnia dostawy Oprogramowania, wykona wdrożenie funkcjonalności zarządzania urządzeniami mobilnymi (MDM), obejmujące:

1) konfigurację umożliwiająca podłączenie/rejestracje urządzeń;
2) konfigurację oraz przygotowanie polityk dla systemów typu Android oraz IOS: root detection, WiFi, szyfrowanie, PIN, profile aplikacji;
3) konfiguracje Portalu Firmy oraz Autopilot;
4) opracowanie i przekazanie dokumentacji (w języku polskim) powdrożeniowej zawierającej polityki, ich konfigurację oraz czynności jakie zostały wykonane krok po kroku wraz z ich dokładnym opisem.

3. Wymagania dotyczące szkoleń:

Wykonawca zapewni przeprowadzenie certyfikowanych szkoleń dla administratorów Zamawiającego zakończonych otrzymaniem certyfikatu uczestnictwa:

Lp.	Kod szkolenia	Nazwa szkolenia	Liczba osób
1.	MS-101T00	Microsoft 365 Mobility and Security *lub równoważne	3

2.	MD-102T00	Microsoft 365 Endpoint Administrator *lub równoważne	3
3.	MS-55399	Implement and Manage Microsoft Intune *lub równoważne	3
4.	MS-55348	Administering Microsoft Endpoint Configuration Manager *lub równoważne	3
5.	SC-200T00	Microsoft Identity and Access Administrator *lub równoważne	3

* w przypadku zaoferowanie oprogramowania równoważnego

Zamawiający dopuszcza zaoferowanie Voucherów umożliwiających udział w szkoleniu, ważnych minimum przez okres 12 miesięcy od dnia zawarcia umowy.

4. Usługa wsparcia technicznego:

Wykonawca zapewni usługę wsparcia technicznego i konsultacje dla zaproponowanego rozwiązania, która będzie realizowana przez co najmniej jednego certyfikowanego specjalistę posiadającą certyfikaty na poziomie: SC-100, SC-400, MS-102, AZ-500, MD-101 lub równoważne certyfikaty dla zaproponowanego rozwiązania. Usługa wsparcia technicznego będzie świadczona w okresie 25 miesięcy od dnia uruchomienia subskrypcji, w wymiarze nie przekraczającym 240 godzin. Usługa wsparcia obejmuje w szczególności:

1) udzielanie konsultacji i wsparcia technicznego;
2) świadczenie pomocy zdalnej administratorom Zamawiającego;
3) obsługę zgłoszeń błędów nieleżących po stronie producenta oprogramowania:
   a) kategorie zgłoszeń błędów:
      – Krytyczny Błąd - wada uniemożliwiająca użytkownikom korzystanie z usługi Microsoft Enterprise Mobility + Security E3 lub jej fragmentu oraz naruszenie bezpieczeństwa usługi Microsoft Enterprise Mobility + Security E3 (dostęp do danych lub funkcji usługi z pominięciem mechanizmów zabezpieczeń),
      – Poważny Błąd - nieprawidłowość działania usługi Microsoft Enterprise Mobility + Security E3, która wpływa w istotny sposób na wyniki pracy, ogranicza funkcjonalność usługi Microsoft Enterprise Mobility + Security E3, w wyniku czego praca jest utrudniona, ale możliwa;
      – Usterka - dysfunkcje, czy uciążliwości utrudniające działanie usługi Microsoft Enterprise Mobility + Security E3.

Wykonawca zobowiązany jest podjąć niezwłocznie po przyjęciu zgłoszenia czynności zmierzające do jego zdiagnozowania oraz podjęcia naprawy, jednak nie później niż w terminach wskazanych poniżej.
O rozpoczęciu diagnozy, wyniku diagnozy oraz podjęciu czynności zmierzających do naprawy błędu lub usterki Wykonawca powiadomi Zamawiającego drogą elektroniczną.

Kategoria zgłoszenia	**Czas Reakcji**[1] (w trybie 24/7/365)	**Czas Naprawy**[2] (w trybie 24/7/365)
Krytyczny błąd	60 min.	2 godz.

[1] Czas podjęcia działań w celu przeprowadzenia diagnostyki i lokalizacji usterki lub błędu.
[2] Czas liczony od chwili potwierdzenia wystąpienia błędu lub usterki do chwili ich usunięcia.

Poważny błąd	2 godz.	4 godz.
Usterka	4 godz.	16 godz.

5. Wymagania dla oprogramowania równoważnego

Opis kryteriów równoważności dla oprogramowania Microsoft Enterprise Mobility + Security E3 stanowi Załącznik nr 1 do SOPZ.

Załącznik nr 1 do SOPZ

Opis wymagań dla oprogramowania równoważnego

1. W przypadku zaoferowania równoważnego produktu, musi on zostać w pełni zintegrowany z obecnie użytkowanymi usługami Microsoft Office 365 E5 oraz aplikacjami Microsoft 365 i musi spełniać następujące wymagania:
   1) Możliwość przypisania administratorów do określonych grup użytkowników lub zasobów;
   2) Tworzenie jednostek administracyjnych dla lepszego zarządzania użytkownikami i zasobami;
   3) Administratorzy widzą tylko użytkowników i zasoby w swojej jednostce;
   4) Administratorzy mogą tworzyć, edytować i usuwać konta tylko w obrębie swojej jednostki;
   5) Możliwość przypisania specyficznych ról administracyjnych dla różnych potrzeb;
   6) Zwiększona kontrola nad danymi użytkowników dla zgodności z regulacjami prawnymi;
   7) Możliwość stosowania różnych polityk dostępu i zabezpieczeń;
   8) Możliwość przypisania polityk zarządzania urządzeniami dla określonych jednostek;
   9) Reguły dynamiczne do automatycznego przypisywania użytkowników do jednostek;
   10) Stosowanie różnych polityk bezpieczeństwa w zależności od jednostki administracyjnej;
   11) Śledzenie działań użytkowników w czasie rzeczywistym dla wykrywania zagrożeń;
   12) Dostarczenie szczegółowych informacji o logowaniach, w tym lokalizacji i urządzeniach;
   13) Identyfikacja nietypowych wzorców zachowań użytkowników;
   14) Automatyczne powiadamianie administratorów o zagrożeniach;
   15) Ocena poziomu ryzyka związana z użytkownikami i ich działaniami;
   16) Monitorowanie urządzeń pod kątem zgodności i potencjalnych zagrożeń;
   17) Łączenie danych z Microsoft Defender i innymi usługami;
   18) Dostęp do archiwalnych incydentów i analiza trendów;
   19) Tworzenie raportów dostosowanych do wymagań organizacji;
   20) Pomoc w spełnianiu wymagań prawnych poprzez dokumentację raportów;
   21) Administratorzy mogą definiować własne atrybuty dla użytkowników, urządzeń i aplikacji w Entra ID;
   22) Możliwość stosowania reguł dostępu opartych na niestandardowych atrybutach użytkowników;
   23) Atrybuty mogą być wykorzystywane w aplikacjach biznesowych zintegrowanych z Azure AD;
   24) Ułatwia klasyfikację użytkowników i automatyzację procesów zarządzania tożsamością;
   25) Możliwość dostosowania zasad dostępu do specyficznych wymagań organizacji;
   26) Niestandardowe atrybuty mogą być używane do automatycznego przypisywania użytkowników do dynamicznych grup;
   27) Atrybuty mogą określać dostęp do określonych aplikacji na podstawie ról użytkowników;
   28) Pomaga w przypisywaniu uprawnień dostępu do systemów i danych;
   29) Dane są przechowywane i szyfrowane w systemie zarządzania tożsamością i dostępem zapewniającym jednokrotne logowanie, uwierzytelnienie wieloskładnikowe oraz ochronę tożsamości użytkowników;
   30) Historia zmian niestandardowych atrybutów jest rejestrowana w celu analizy i zgodności;
   31) Administratorzy mogą dostosować stronę logowania, dodając logo firmy, tło i komunikaty;
   32) Możliwość wyświetlania różnych elementów graficznych w zależności od użytkownika lub organizacji B2B;

33) Poprawia rozpoznawalność firmy i zmniejsza ryzyko ataków phishingowych poprzez unikalny wygląd strony logowania;
34) Możliwość dodania wiadomości o politykach firmy lub procedurach logowania;
35) Wsparcie dla różnych języków w komunikatach logowania użytkowników międzynarodowych;
36) Administratorzy mogą dodawać niestandardowe linki do pomocy technicznej i polityk bezpieczeństwa;
37) Personalizowana strona logowania może być wyświetlana w zależności od polityk dostępu warunkowego;
38) Strona logowania wspiera różne metody wieloskładnikowego uwierzytelniania (MFA);
39) Możliwość przekierowywania użytkowników na niestandardowe strony po wylogowaniu;
40) Personalizowana strona logowania działa również dla aplikacji hybrydowych;
41) Użytkownicy i urządzenia są dynamicznie przypisywane do grup na podstawie atrybutów, np. działu czy stanowiska;
42) Oszczędza czas administratorów, automatycznie aktualizując członkostwo grupy przy zmianach w katalogu;
43) Dynamiczne grupy można wykorzystać w systemie zarządzania urządzeniami, systemie zarządzania tożsamością oraz dostępie warunkowym;
44) Automatycznie przypisuje użytkowników do odpowiednich grup zabezpieczeń;
45) Minimalizuje błędy wynikające z ręcznego dodawania użytkowników do grup;
46) Reguły dynamiczne mogą wykorzystywać atrybuty użytkownika, takie jak rola czy lokalizacja;
47) Grupy są aktualizowane w czasie rzeczywistym na podstawie zmian w katalogu użytkowników;
48) Dynamiczne grupy mogą służyć do zarządzania politykami urządzeń;
49) Możliwość dynamicznego grupowania urządzeń na podstawie ich właściwości;
50) Dynamiczne grupy mogą automatycznie przypisywać licencje do użytkowników spełniających określone kryteria;
51) Śledzi wydajność i kondycję serwerów AD oraz synchronizacji Azure AD Connect;
52) Automatyczne powiadomienia o problemach z synchronizacją katalogu lub AD FS;
53) Możliwość przesyłania danych o stanie systemu do SIEM lub narzędzi analitycznych;
54) Analizuje błędy logowania użytkowników w hybrydowym środowisku tożsamości;
55) Wykrywa podejrzane działania związane z synchronizacją tożsamości;
56) Monitoruje szybkość i dokładność synchronizacji katalogu użytkowników;
57) Przechowuje logi synchronizacji dla celów analizy i audytu;
58) Możliwość wykrywania ataków na Active Directory dzięki połączeniu z Microsoft Defender for Identity;
59) Monitorowanie i raportowanie w środowiskach z wieloma serwerami AD Connect;
60) Administracja dostępem do systemów na podstawie kondycji katalogu;
61) Umożliwia organizacjom zarządzanie dostępem partnerów, dostawców i klientów;
62) Obsługuje logowanie przez konta Microsoft, Google, Facebook i innych dostawców;
63) Partnerzy mogą korzystać z firmowych aplikacji bez konieczności tworzenia kont wewnętrznych;
64) Ułatwia dostęp do firmowych usług dla zewnętrznych użytkowników;
65) Wspiera OpenID Connect, SAML i OAuth;
66) Administratorzy mogą dostosować ścieżki uwierzytelniania dla różnych grup użytkowników;
67) Możliwość stosowania polityk dostępu warunkowego dla użytkowników zewnętrznych;
68) Śledzenie logowań i operacji wykonywanych przez użytkowników zewnętrznych;

69) Zapewnienie dodatkowego poziomu zabezpieczeń dla dostępu spoza organizacji;
70) Automatyzacja tworzenia i usuwania kont dla partnerów biznesowych;
71) Zarządza tożsamościami między AD, Azure AD i innymi systemami tożsamości;
72) Tworzy, aktualizuje i usuwa konta użytkowników na podstawie źródeł HR;
73) Chroni konta uprzywilejowane i zapobiega nadużyciom;
74) Umożliwia przypisywanie użytkowników do ról z określonymi uprawnieniami;
75) Umożliwia użytkownikom resetowanie haseł zgodnie z polityką firmy;
76) Obsługuje synchronizację tożsamości z systemami onpremises;
77) Możliwość synchronizacji tożsamości pomiędzy lokalnym AD a Azure AD;
78) Generuje raporty o aktywności użytkowników i zmianach w katalogu;
79) Zapewnia audyty i raporty zgodności dotyczące dostępu użytkowników;
80) Umożliwia zarządzanie użytkownikami przez różne działy w organizacji;
81) Zapobiega używaniu łatwych do odgadnięcia haseł, np. „Password123”;
82) Organizacja może dodawać własne słowa kluczowe do listy zabronionych haseł;
83) Możliwość egzekwowania tych samych zasad hasła w lokalnym Active Directory;
84) Identyfikuje ryzykowne schematy zmian haseł i ostrzega użytkowników;
85) Blokowanie ponownego użycia wcześniejszych haseł użytkownika;
86) Użytkownicy otrzymują alerty, gdy ich hasło wymaga zmiany z powodów bezpieczeństwa;
87) Analizuje hasła pod kątem naruszeń danych i zgłasza konieczność ich zmiany;
88) Komunikaty o naruszeniach haseł są dostosowane do języka użytkownika;
89) Zasady dotyczące haseł mogą być powiązane z regułami Conditional Access;
90) Zapewnia raporty dotyczące przestrzegania polityk haseł w organizacji;
91) Użytkownicy mogą logować się za pomocą kluczy FIDO2, aplikacji Authenticator lub Windows Hello;
92) Integracja z Windows Hello for Business umożliwia logowanie biometryczne;
93) Możliwość logowania za pomocą fizycznych kluczy sprzętowych zgodnych z FIDO2;
94) Logowanie za pomocą aplikacji Authenticator zamiast hasła;
95) Logowanie na podstawie jednorazowych kodów SMS (jeśli organizacja pozwala);
96) Weryfikuje lokalizację, urządzenie i inne czynniki, aby zatwierdzić logowanie;
97) Możliwość stosowania polityk dostępowych dla metod bezhasłowych;
98) Hasła nie są używane, więc niemożliwe jest ich wykradzenie przez phishing;
99) Działa na systemach Windows, macOS i Linux;
100) Eliminuje konieczność pamiętania skomplikowanych haseł;
101) Pozwala użytkownikom na samodzielne resetowanie haseł bez konieczności angażowania działu IT;
102) Synchronizuje zmiany haseł z lokalnym Active Directory i Azure AD;
103) Resetowanie hasła może wymagać dodatkowej weryfikacji, np. kodu SMS lub aplikacji Authenticator;
104) Administratorzy mogą określać reguły dotyczące częstotliwości resetowania i wymagań dotyczących haseł;
105) Użytkownicy mogą resetować hasła także przez aplikacje mobilne Microsoft;
106) Administratorzy mają dostęp do szczegółowych logów dotyczących resetowania haseł;
107) Resetowanie hasła może wymagać użycia wieloskładnikowego uwierzytelniania dla dodatkowego bezpieczeństwa;

108) Użytkownicy mogą otrzymywać powiadomienia e-mail o zmianie hasła;
109) System może wykrywać podejrzane żądania resetu hasła i blokować je;
110) Reset hasła można wymusić tylko dla określonych grup użytkowników lub urządzeń;
111) Administratorzy mogą śledzić zmiany haseł, logowania i inne operacje wykonane przez użytkowników;
112) Udostępnia szczegółowe raporty o logowaniach użytkowników, w tym lokalizacje i adresy IP;
113) Możliwość identyfikowania, którzy użytkownicy posiadają dostęp do określonych aplikacji i zasobów;
114) Możliwość wykrywania podejrzanej aktywności w kontekście zagrożeń cyberbezpieczeństwa;
115) Administratorzy mogą eksportować dane do formatu CSV lub integrować je z systemami SIEM;
116) Wykrywanie podejrzanych działań, np. wielokrotnych prób logowania z różnych lokalizacji;
117) Konfigurowalne powiadomienia o podejrzanych zdarzeniach związanych z tożsamością użytkownika;
118) System analizuje ryzyko dla poszczególnych kont użytkowników i administratorów;
119) Raporty mogą być wykorzystywane do automatycznego zarządzania dostępem użytkowników;
120) Pomaga organizacjom w przestrzeganiu regulacji dotyczących zarządzania tożsamościami i bezpieczeństwa danych;
121) System automatycznie zmienia hasła współdzielonych kont aplikacji, zwiększając bezpieczeństwo;
122) Użytkownicy mogą logować się do aplikacji bez znajomości rzeczywistego hasła;
123) Możliwość stosowania rotacji haseł w połączeniu z SSO dla aplikacji SaaS;
124) System obsługuje zarówno aplikacje on-premises, jak i te w chmurze;
125) Administratorzy mogą określić, jak często hasła powinny być automatycznie zmieniane;
126) Śledzenie, kto i kiedy uzyskał dostęp do współdzielonych kont;
127) Automatyczna zmiana haseł może być wymuszana zgodnie z politykami organizacji;
128) Możliwość stosowania w różnych systemach, np. bazach danych, VPN i aplikacjach SaaS;
129) Hasła mogą być dostępne tylko dla upoważnionych użytkowników w sposób zaszyfrowany;
130) Administratorzy mogą przeglądać historię użycia współdzielonych kont i ich haseł;
131) Umożliwia użytkownikom jednokrotne logowanie do różnych aplikacji SaaS bez konieczności ponownego uwierzytelniania;
132) Obsługuje standardowe protokoły federacyjne, zapewniając kompatybilność z wieloma aplikacjami;
133) Pozwala na automatyczne tworzenie i usuwanie kont w aplikacjach SaaS na podstawie statusu użytkownika;
134) Administratorzy mogą definiować, które grupy użytkowników mają dostęp do określonych aplikacji;
135) Dostęp do aplikacji SaaS można ograniczać na podstawie urządzenia, lokalizacji czy poziomu ryzyka logowania;
136) Pozwala administratorom na monitorowanie i kontrolowanie logowań do aplikacji SaaS;
137) Zapewnia jednokrotne logowanie do aplikacji działających zarówno w chmurze, jak i lokalnie;
138) Śledzi aktywność użytkowników i wykrywa podejrzane próby logowania;
139) Zapewnia natywną obsługę SSO dla aplikacji Microsoft 365;
140) Łączy logowanie do aplikacji SaaS i on-premises w ramach jednego katalogu tożsamości;
141) Pozwala użytkownikom na logowanie bez hasła, używając jednorazowego kodu wysyłanego na telefon;
142) Umożliwia logowanie do systemu za pomocą SMS-ów;
143) Nie wymaga specjalnych aplikacji – użytkownik wprowadza tylko swój numer telefonu;
144) Może być stosowane jako metoda MFA w połączeniu z innymi mechanizmami uwierzytelniania;

145) Może być używane do logowania do aplikacji wewnętrznych organizacji;
146) Idealne dla pracowników kontraktowych, którzy nie mają konta stałego;
147) Administratorzy mogą zdefiniować, którzy użytkownicy mogą korzystać z SMS Sign-in;
148) Rejestruje próby logowania i wykrywa potencjalnie podejrzane działania;
149) Użytkownicy mogą korzystać z SMS Sign-in na telefonach i tabletach;
150) Nie wymaga wpisywania haseł, co zmniejsza ryzyko ich wykradzenia;
151) Pozwala administratorom generować tymczasowe kody dostępu dla użytkowników;
152) Można używać jako alternatywy dla tradycyjnych haseł;
153) Użytkownicy mogą wykorzystać kod do rejestracji aplikacji Authenticator;
154) Ułatwia dostęp użytkownikom, którzy utracili dostęp do metod uwierzytelniania;
155) Może być stosowane do przywracania dostępu administratorom w sytuacjach awaryjnych;
156) Może działać jako tymczasowa metoda wieloskładnikowego uwierzytelniania;
157) Administratorzy mogą określić czas, po którym kod wygasa;
158) Nowi pracownicy mogą użyć Temporary Access Pass do pierwszego logowania;
159) Użytkownicy mogą dodawać nowe urządzenia bez pomocy administratora;
160) Kody są unikalne i nie mogą być ponownie używane po wykorzystaniu;
161) Pozwala użytkownikom na udostępnianie zweryfikowanych informacji bez udostępniania nadmiarowych danych;
162) Działa w oparciu o technologię blockchain i zdecentralizowaną tożsamość;
163) Firmy mogą wymagać Verified ID do potwierdzenia tożsamości użytkowników przed udzieleniem dostępu;
164) Chroni dane osobowe poprzez minimalizację udostępnianych informacji;
165) Może być używane do potwierdzania dokumentów tożsamości;
166) Możliwość stosowania Verified ID jako dodatkowej metody uwierzytelniania;
167) Użytkownicy mogą zapisywać swoje Verified ID na telefonie;
168) Spełnia wymagania dotyczące ochrony danych osobowych (np. GDPR);
169) Pozwala użytkownikom logować się do usług online bez konieczności tworzenia nowego konta;
170) Umożliwia integrację z rozwiązaniami MFA firm trzecich, takimi jak Duo Security czy Okta;
171) Pozwala na autoryzację użytkowników za pomocą zewnętrznych usług uwierzytelniania;
172) MFA od dostawców zewnętrznych może być stosowane w politykach Conditional Access;
173) Obsługuje MFA w połączeniu z aplikacjami SaaS i systemami on-premises;
174) Zewnętrzne MFA może być wykorzystywane do zabezpieczania połączeń VPN;
175) Obsługuje użytkowników korzystających zarówno z lokalnego AD, jak i Azure AD;
176) Administratorzy mogą określać, kiedy wymagana jest dodatkowa weryfikacja;
177) Monitoruje i zapisuje wszystkie próby uwierzytelnienia wieloskładnikowego;
178) Integracja z kluczami FIDO2 i innymi metodami uwierzytelniania;
179) Zewnętrzne MFA może być stosowane również dla partnerów biznesowych;
180) Administratorzy mogą kontrolować, które aplikacje są dostępne dla określonych użytkowników;
181) Ułatwia tworzenie, aktualizowanie i usuwanie kont użytkowników w aplikacjach SaaS;
182) Umożliwia jednokrotne logowanie do wszystkich aplikacji firmowych;
183) Zapewnia raporty dotyczące wykorzystania aplikacji w organizacji;

184) Możliwość zarządzania dostępem zarówno do aplikacji SaaS, jak i on-premises;
185) Administratorzy mogą definiować polityki dostępu oparte na typie urządzenia;
186) Użytkownicy mogą korzystać z zarządzanych aplikacji na smartfonach i tabletach;
187) Pozwala na zabezpieczanie danych aplikacji mobilnych i komputerowych;
188) Dostęp do aplikacji można ograniczać na podstawie lokalizacji, urządzenia i innych parametrów;
189) Identyfikuje aplikacje używane w organizacji bez oficjalnej autoryzacji;
190) Administratorzy mogą rejestrować urządzenia i przypisywać im polityki dostępu;
191) Możliwość wymuszania zasad bezpieczeństwa na urządzeniach użytkowników;
192) Administratorzy mogą sprawdzać, czy urządzenia spełniają wymagania organizacyjne;
193) Wszystkie zarządzane urządzenia mogą być zabezpieczane szyfrowaniem BitLocker;
194) Możliwość usunięcia danych firmowych z urządzenia w przypadku jego utraty;
195) Pozwala na pełne zarządzanie urządzeniami mobilnymi i komputerami;
196) Zapewnia bezpieczny dostęp do firmowych zasobów na prywatnych urządzeniach użytkowników;
197) Administratorzy mogą przeglądać szczegółowe raporty dotyczące zarządzanych urządzeń;
198) Możliwość zdalnego wdrażania firmowych aplikacji na urządzenia użytkowników;
199) Analiza potencjalnych zagrożeń i podejrzanej aktywności na urządzeniach;
200) Umożliwia szyfrowanie i kontrolę dostępu do poufnych informacji organizacji;
201) Administratorzy mogą definiować, kto może odczytywać, edytować lub drukować dokumenty;
202) Pozwala użytkownikom zabezpieczać dokumenty Word, Excel i PowerPoint bezpośrednio z aplikacji;
203) Chroni załączniki i treści wiadomości e-mail przed nieautoryzowanym dostępem;
204) Zapewnia ochronę dokumentów przechowywanych w bibliotekach SharePoint;
205) Pliki pozostają zaszyfrowane nawet po opuszczeniu infrastruktury organizacji;
206) Możliwość definiowania zasad dostępu na podstawie grup użytkowników i ról;
207) Możliwość implementacji zarówno w środowiskach onpremises, jak i w chmurze;
208) Pomaga organizacjom spełniać wymagania dotyczące ochrony danych, np. GDPR;
209) Administratorzy mogą śledzić, kto i kiedy otwierał zabezpieczone pliki;
210) Monitoruje i analizuje zachowania użytkowników oraz urządzeń w celu identyfikacji zagrożeń;
211) System wykrywa anomalia i potencjalne ataki na infrastrukturę IT;
212) ATA analizuje ruch sieciowy i zachowanie użytkowników w AD, aby wykrywać zagrożenia;
213) Identyfikuje nieautoryzowane próby przejęcia kont użytkowników;
214) Administratorzy otrzymują alerty o potencjalnych atakach w organizacji;
215) Porównuje działania użytkowników z ich standardowymi wzorcami pracy, wykrywając anomalie;
216) Zapewnia szczegółowe raporty o potencjalnych zagrożeniach bezpieczeństwa;
217) Możliwość eksportowania danych do systemów zarządzania zdarzeniami bezpieczeństwa;
218) Identyfikuje podejrzane działania użytkowników z uprawnieniami administratora;
219) Działa zarówno w chmurze, jak i lokalnych infrastrukturach IT;
220) Umożliwia szyfrowanie i kontrolę dostępu do plików przechowywanych w Microsoft 365 i OneDrive;
221) Chroni wiadomości e-mail, zapewniając dostęp tylko autoryzowanym odbiorcom;
222) Zapewnia dodatkowe funkcje klasyfikacji i etykietowania dokumentów;
223) Administratorzy mogą określać, kto i jak długo może otwierać zaszyfrowane pliki;

224) Śledzi aktywność użytkowników w odniesieniu do zabezpieczonych dokumentów;
225) Dostęp do zaszyfrowanych danych można ograniczyć na podstawie lokalizacji czy urządzenia;
226) Użytkownicy mogą otwierać zabezpieczone pliki na urządzeniach mobilnych;
227) Zabezpiecza dokumenty przed kopiowaniem i nieautoryzowanym udostępnianiem;
228) Chroni pliki udostępniane w SharePoint przed nieautoryzowanym dostępem;
229) Pomaga organizacjom przestrzegać regulacji dotyczących ochrony danych, np. HIPAA, GDPR;
230) Pozwala administratorom na centralne zarządzanie konfiguracją systemów Windows w organizacji;
231) Umożliwia wdrażanie i aktualizowanie aplikacji na komputerach użytkowników;
232) Sprawdza, czy urządzenia spełniają wymagania organizacyjne dotyczące polityk bezpieczeństwa;
233) Administratorzy mogą konfigurować urządzenia bez konieczności fizycznego dostępu;
234) Umożliwia współpracę z rozwiązaniami chmurowymi do zarządzania urządzeniami mobilnymi;
235) Możliwość zarządzania komputerami z Windows, macOS i Linux;
236) Zapewnia wsparcie dla skryptów PowerShell i innych metod automatyzacji;
237) Zapewnia szczegółowe raporty dotyczące stanu systemów w organizacji;
238) Pozwala administratorom wymuszać określone polityki na zarządzanych urządzeniach;
239) Analizuje wydajność systemów i pomaga w optymalizacji konfiguracji sprzętu;
240) Zapewnia zabezpieczenia antywirusowe i antymalware dla urządzeń końcowych;
241) Monitoruje i wykrywa podejrzane działania na komputerach użytkowników;
242) Łączy się z Defender for Endpoint w celu zaawansowanej ochrony;
243) Pozwala administratorom definiować, które aplikacje mogą być uruchamiane na urządzeniach;
244) Monitoruje nietypowe zachowania użytkowników w celu identyfikacji potencjalnych zagrożeń;
245) Automatycznie analizuje nieznane pliki i blokuje potencjalnie szkodliwe oprogramowanie;
246) Automatycznie izoluje urządzenia wykazujące podejrzane aktywności, aby zapobiec rozprzestrzenianiu się ataków;
247) Administratorzy mogą konfigurować polityki zabezpieczeń dla całej organizacji;
248) Generuje szczegółowe raporty dotyczące prób ataków i naruszeń bezpieczeństwa;
249) Chroni urządzenia przed nowymi zagrożeniami, korzystając z aktualizacji baz sygnatur;
250) Zapewnia administratorom dane o stanie i wydajności urządzeń końcowych;
251) Analizuje czas uruchamiania systemów i aplikacji, wykrywając potencjalne spowolnienia;
252) Sugeruje administratorom zmiany w konfiguracji systemów w celu poprawy ich wydajności;
253) Zbiera informacje o błędach systemowych i aplikacyjnych w organizacji;
254) Śledzi, jak użytkownicy korzystają z urządzeń i aplikacji;
255) Umożliwia monitorowanie i optymalizację urządzeń zarządzanych przez system MDM, zapewniający zgodność z polityki bezpieczeństwa, analizę wydajności oraz automatyzację konfiguracji;
256) Analizuje, czy urządzenia są zgodne z najnowszymi wymaganiami systemowymi;
257) Pozwala administratorom analizować różnice w wydajności między różnymi działami;
258) Umożliwia szybkie wykrywanie problemów zgłaszanych przez pracowników;
259) Pomaga w identyfikacji nieefektywnie wykorzystywanych urządzeń i aplikacji;
260) Pozwala organizacjom oznaczać i kategoryzować dane na podstawie ich poufności;
261) Zapewnia automatyczne szyfrowanie plików i dokumentów na podstawie zasad organizacji;

262) Śledzi, kto i kiedy uzyskał dostęp do poufnych plików;
263) Administratorzy mogą definiować zasady dotyczące ochrony i udostępniania danych;
264) Działa z aplikacjami Office 365, takimi jak Outlook, Word i Excel.
265) Zapewnia kontrolę nad udostępnianiem plików w OneDrive, SharePoint i innych usługach chmurowych;
266) Blokuje przesyłanie poufnych informacji poza organizację;
267) Umożliwia zarządzanie kluczami szyfrowania i zabezpieczeniem treści;
268) Rejestruje wszystkie działania związane z dostępem i edycją zabezpieczonych plików;
269) Pomaga organizacjom spełniać wymagania zgodności, takie jak GDPR i HIPAA;
270) Web portal dostępny przez HTTPS;
271) Web portal musi być tworzony zgodnie z zaleceniami standardu OWASP - TOP 10 (Open Web Application Security Project) lub podobnego;
272) Przesył danych musi być szyfrowany. Dane przesyłane do i z oferowanego rozwiązania muszą być przesyłane w sposób bezpieczny zapewniając przesyłanym danym integralność oraz poufność (szyfrowanie za pomocą bezpiecznych protokołów tj. min. TLS 1.2 przy użyciu silnych algorytmów szyfrowania minimum AES 256 bits i długości klucza RSA 2048 bits);
273) Przypisywanie ról na podstawie Role-based Access Control: (np. administrator, helpdesk, operator);
274) Portal musi umożliwiać administratorowi przeglądanie historii logowania użytkowników;
275) Interfejs dostępny co najmniej w języku polskim i angielskim;
276) Możliwość wymuszenia logowania MFA (Multi Factor Authenticator) dla administratorów;
277) Portal musi zapewniać możliwość definitywnego usunięcia danych osobowych;
278) Przechowywane dane identyfikujące oraz uwierzytelniające w spoczynku w zintegrowanych/powiązanych z Portalem aplikacjach muszą być zabezpieczone przed niepowołanym odczytaniem (np. poprzez szyfrowanie);
279) Wykonawca zapewnienia ochronę antywirusową oprogramowania, włączając w to oprogramowanie Anti-Spam/Malware/Antivirus w zakresie ochrony usługi;
280) Obsługiwane platformy: iOS 16.0 i wyższy, Android OS 10.0 i wyższy, macOS, Windows 10/11, Linux;
281) Polityki bezpieczeństwa: Hasła i blokada ekranu, Wymuszenie typu i złożoności, PIN/hasła do urzadzenia mobilnego, limit prób, po którym urządzenie mobilne zostaje zablokowane, ustawianie blokady poprzez politykę/regułę: kamera, bluetooth, NFC, USB debugging mode, instalacja aplikacji spoza sklepu Play/App Store, nieuprawniony jailbreak / rooting, możliwość ustawienia oddzielnego kontenera na urządzeniach mobilnych (tylko dane służbowe w zaszyfrowanym kontenerze/folderze), Conditional Access: ograniczenie dostępu do zasobów wg lokalizacji, stanu urządzenia, grup użytkowników;
282) Zarządzanie aplikacjami: Deployment: zdalna instalacja aplikacji firmowych i ze sklepów (Apple App Store, Google Play), White/black listing: tworzenie dozwolonych i blokowanych list aplikacji, OTA Updates: zarządzanie aktualizacjami aplikacji, Firmowy sklep: Możliwość ustawienia Company Portal jako „sklepu" dla zatwierdzonych aplikacji, Kiosk / Single App Mode dla urządzeń z systemem Android;
283) Monitoring i raportowanie: zbierane dane: wersja OS, zainstalowane aplikacje i ich wersje, stan pamięci i baterii, identyfikatory IMEI, numer seryjny, raporty: wbudowane szablony (CSV, PDF), możliwość eksportu danych i harmonogramowania wysyłki mailowej, alerty: powiadomienia o niezgodnościach z politykami, braku kontaktu z urzadzeniem itp., Integracja z SIEM: poprzez Azure Monitor/Log Analytics lub API Graph.

2. W przypadku zaoferowania subskrypcji na oprogramowanie równoważne oferowane szkolenia muszą spełniać następujące wymagania:
   1) zakresem, tematyką oraz formą odpowiadają szkoleniom Microsoft, o których mowa w pkt 4 SOPZ i dotyczą zaoferowanego oprogramowania;
   2) czas trwania szkoleń odpowiada czasowi trwania szkoleń Microsoft, o których mowa w pkt 4 SOPZ;
   3) zakres materiałów szkoleniowych dla uczestników szkoleń odpowiada zakresowi materiałów szkoleń Microsoft, o których mowa w pkt 4 SOPZ.