Omówienie wdrażania komputerów Mac

Wprowadzenie

Spis treści

Jesteśmy przekonani, że pracownicy każdej organizacji będą mogli w pełni pokazać, na co ich stać, gdy zapewni im się dostęp do najlepszych narzędzi i rozwiązań technicznych. Wszystkie produkty Apple projektowane są w taki sposób, by dzięki nim pracownicy byli bardziej kreatywni i wydajni oraz by poszukiwali nowych sposobów pracy — czy to w biurze, czy w podróży. Ponieważ pracownicy tak właśnie chcą pracować we współczesnym świecie. Oczekują lepszego dostępu do informacji, warunków do bezproblemowej pracy zespołowej i dzielenia się informacjami, a także swobodnej łączności i możliwości wyboru miejsca pracy.

Przygotowywanie komputerów Mac i wdrażanie ich we współczesnym środowisku biznesowym nigdy jeszcze nie było tak proste. Kluczowe usługi Apple wraz z rozwiązaniem innej firmy do zarządzania urządzeniami mobilnymi (Mobile Device Management, MDM) umożliwiają organizacji bezproblemowe wdrożenie komputerów Mac na odpowiednią skalę, a potem zapewnienie wsparcia użytkownikom tych urządzeń. Jeśli w organizacji przeprowadzono już wewnętrzne wdrożenie urządzeń z systemami iOS i iPadOS, to prawdopodobnie przy tamtej okazji wykonano też większość prac przygotowujących infrastrukturę do implementacji systemu macOS.

Wprowadzone niedawno udoskonalenia w dziedzinie bezpieczeństwa i wdrażania komputerów Mac oraz zarządzania nimi umożliwiają organizacji przejście od monolitycznego systemu obrazów instalacyjnych i tradycyjnego powiązania z katalogiem na rzecz modelu swobodnego udostępniania i wdrażania zasobów, stawiającego potrzeby użytkownika na pierwszym miejscu i realizowanego niemal wyłącznie za pomocą narzędzi wbudowanych w system macOS.

Niniejszy dokument zawiera wskazówki na temat wszystkich aspektów wdrażania komputerów Mac na większą skalę: od analizy istniejącej infrastruktury, poprzez zarządzanie urządzeniami, aż po swobodne udostępnianie zasobów. Zagadnienia uwzględnione w niniejszym dokumencie są opisane bardziej szczegółowo w podręczniku wdrażania komputerów Mac, dostępnym w Internecie pod adresem: support.apple.com/guide/deployment-reference-macos

Pierwsze kroki

W początkowej fazie procesu wdrażania ważne jest opracowanie strategii wdrożenia i planu realizacji, a także analiza obecnej charakterystyki wykorzystania systemu macOS przez pracowników. Należy zadbać o to, aby właściwe zespoły odpowiednio wcześnie zaangażowały się we wdrożenie, oraz zwracać uwagę na zgodność planów i działań z wizją oraz celami organizacji. Niektóre zespoły zaczynają od małego dowodu poprawności rozwiązania, który ujawni trudności specyficzne dla konkretnego środowiska. Zaangażowanie dotychczasowych użytkowników w szerszy program pilotażowy jest bardzo ważne, ponieważ pozwala zorientować się, jak urządzenia są faktycznie używane w organizacji i czy zespół wdrożeniowy powinien zwrócić uwagę na jakieś problemy.

Informacje zebrane w tej fazie mogą pomóc w ustaleniu, które role i funkcje potencjalnie odniosą największe korzyści z wdrożenia komputerów Mac. Następnie dział IT może ocenić, czy system macOS powinien być oferowany pracownikom w całej organizacji jako standardowe wyposażenie, czy też jako opcja do wyboru dla osób realizujących niektóre funkcje.

Często w tej fazie powstaje też obszerna lista wewnętrznych aplikacji i narzędzi, których kompatybilność z platformą Mac musi być zapewniona, zanim platforma ta zostanie wdrożona na szeroką skalę. Należy tutaj skupić się na podstawowych aplikacjach biurowych oraz aplikacjach wspomagających pracę grupową i komunikację. Dostępność tych aplikacji zaspokoi potrzeby większości użytkowników. Newralgiczne usługi wewnętrzne, takie jak firmowy intranet, katalog i oprogramowanie do zarządzania wydatkami, również mają znaczenie dla produktywności pracy dużych obszarów organizacji.

Należy udokumentować wszelkie obejścia i alternatywy dla pozostałych narzędzi wewnętrznych oraz opublikować informacje o nich, jednocześnie zachęcając osoby i jednostki odpowiedzialne za aplikacje do ich modernizacji. Ważna jest przejrzystość w informowaniu użytkowników o aplikacjach biznesowych, z których będą mogli korzystać, jeśli wybiorą Maca, a ustalając priorytety prac modernizacyjnych należy kierować się oczekiwaniami użytkowników. Gdy wystąpi taka potrzeba, należy wspólnie z osobami i jednostkami odpowiedzialnymi za aplikacje opracować plan uaktualnień, zakładając wykorzystanie zestawu macOS SDK i języka Swift, a także pomoc firm partnerskich w pracach programistycznych.

Powszechnie spotykanym modelem jest udostępnianie pracownikom komputerów Mac stanowiących własność firmy. Niektóre przedsiębiorstwa mogą zezwalać pracownikom na używanie prywatnych Maców w pracy, w ramach programów BYOD (bring-your-own-device). Niezależnie od modelu własności zaoferowanie użytkownikom produktów Apple do wyboru może przynieść korzyści w skali całej organizacji, takie jak: wyższy poziom produktywności, kreatywności, zaangażowania pracowników i ich zadowolenia z pracy, a także niższe koszty po uwzględnieniu wartości rezydualnej i kosztów wsparcia. Organizacje mają też do dyspozycji różne warianty leasingu i finansowania, dzięki którym nie muszą już na samym początku ponosić wysokich kosztów. Organizacje mogą również kompensować koszty poprzez partycypację pracowników, np. oferując wymianę sprzętu na nowszy w zamian za potrącenie części wynagrodzenia lub umożliwiając pracownikom wykup sprzętu poleasingowego lub wycofywanego.

Zasady obowiązujące w firmie, a także procesy wdrożenia, zarządzania i wsparcia opisane w tym dokumencie, mogą różnić się w zależności od informacji zgromadzonych podczas projektu pilotażowego. Stuprocentowa unifikacja zasad, ustawień i aplikacji u wszystkich użytkowników nie musi być dobrym rozwiązaniem, ponieważ wymagania różnych grup i zespołów w firmie często bardzo się różnią.

Etapy wdrażania

Proces wdrażania systemu macOS można podzielić na cztery główne kroki: przygotowanie środowiska, skonfigurowanie systemu MDM, wdrożenie urządzeń wśród pracowników, a następnie wykonywanie bieżących zadań zarządzania.

1. Przygotowanie

Każde wdrożenie powinno rozpocząć się od przygotowania już istniejącego środowiska. Ta faza obejmuje pogłębioną analizę sieci i najważniejszych składników infrastruktury, a także przygotowanie systemów potrzebnych do pomyślnego wdrożenia.

Ocena istniejącej infrastruktury

Choć komputery Mac dają się bezproblemowo zintegrować z większością standardowych korporacyjnych środowisk IT, ważnym zadaniem pozostaje ocena istniejącej infrastruktury pod kątem optymalnego wykorzystania wszystkich możliwości i zalet systemu macOS. Jeśli organizacja potrzebuje pomocy w przeprowadzeniu takiej oceny, może skorzystać ze wsparcia działu Apple Professional Services lub zwrócić się do zespołu technicznego jednego z naszych partnerów handlowych lub sprzedawców.

Wi-Fi i sieć

Stabilny, niezawodny dostęp do sieci bezprzewodowej jest niezbędny do konfigurowania urządzeń z systemem macOS. Należy zweryfikować projekt firmowej sieci Wi-Fi pod kątem pojemności oraz obsługi przemieszczających się urządzeń. W szczególności starannie rozważyć trzeba rozmieszczenie punktów dostępu i ich moc.

Jeśli urządzenia nie mogą uzyskać dostępu do serwerów Apple, korzystać z usługi powiadomień w trybie push firmy Apple (Apple Push Notification service, APNs), iCloud lub iTunes Store, konieczne może być również zmodyfikowanie konfiguracji proxy WWW lub portów zapór. Podobnie jak w przypadku urządzeń iPad i iPhone, niektóre elementy procesu wdrożenia komputerów Mac — zwłaszcza ich nowszych modeli — wymagają stabilnego dostępu do tych usług w celu wykonania takich czynności, jak uaktualnienie oprogramowania sprzętowego podczas instalacji.

Firmy Apple i Cisco zoptymalizowały komunikację komputerów Mac z siecią bezprzewodową Cisco, w szczególności zapewniając obsługę zaawansowanych funkcji sieciowych systemu macOS, takich jak zarządzanie jakością usług (Quality of Service, QoS). Jeśli firma używa sprzętu sieciowego marki Cisco, to należy zwrócić się do zespołu odpowiedzialnego za sieć, by zadbał o możliwość optymalizacji newralgicznego ruchu z i do komputerów Mac.

Konieczna jest także ocena infrastruktury VPN w celu zapewnienia użytkownikom zabezpieczonego zdalnego dostępu do zasobów firmowych. Warto rozważyć użycie funkcji VPN na żądanie w systemie macOS, tak aby połączenie VPN było nawiązywane tylko wtedy, gdy jest potrzebne. Jeżeli bramy VPN mają obsługiwać osobne połączenia z poszczególnych aplikacji, należy je odpowiednio skonfigurować i zakupić tyle licencji, by zaspokoić potrzeby planowanej liczby użytkowników i połączeń.

Konfiguracja infrastruktury sieciowej powinna umożliwiać korzystanie z usługi Bonjour — opartego na standardach, niewymagającego konfiguracji protokołu sieciowego opracowanego przez Apple. Bonjour umożliwia urządzeniom automatyczne znajdowanie usług w sieci. System macOS używa Bonjour do nawiązywania połączeń z drukarkami obsługującymi funkcję AirPrint, a także z urządzeniami zgodnymi z funkcją AirPlay, takimi jak Apple TV. Niektóre aplikacje i wbudowane funkcje systemu macOS mogą także za pośrednictwem Bonjour odnajdywać inne urządzenia, umożliwiając użytkownikom współpracę i wymianę plików.

Więcej informacji o projektowaniu sieci Wi-Fi:
support.apple.com/guide/deployment-reference-macos

Więcej informacji o konfigurowaniu sieci na potrzeby rozwiązania MDM:
support.apple.com/HT210060

Więcej informacji o protokole Bonjour:
support.apple.com/guide/deployment-reference-macos

Zarządzanie tożsamościami

System macOS może korzystać z usług katalogowych służących do zarządzania tożsamościami i innymi danymi użytkowników, w tym z usług Active Directory, Open Directory oraz LDAP. Niektórzy dostawcy rozwiązań MDM udostępniają gotowe narzędzia do ich integracji z katalogami Active Directory i LDAP. Dodatkowe narzędzia, takie jak rozszerzenie do pojedynczego logowania Kerberos w systemie macOS Catalina, umożliwiają integrację z zasadami i funkcjami usługi Active Directory bez konieczności stosowania tradycyjnych powiązań i kont przenośnych. Rozwiązanie MDM może również zarządzać różnego typu certyfikatami wystawianymi przez wewnętrzne i zewnętrzne urzędy certyfikacji (Certificate Authorities, CA), tak by tożsamości automatycznie były zaufane.

Więcej informacji o nowym rozszerzeniu do pojedynczego logowania Kerberos:
support.apple.com/guide/deployment-reference-macos

Więcej informacji o integracji z usługami katalogowymi:
support.apple.com/guide/deployment-reference-macos

Podstawowe usługi dla pracowników

Należy upewnić się, że wdrożona w przedsiębiorstwie usługa Microsoft Exchange jest aktualna i skonfigurowana tak, by obsługiwała wszystkich użytkowników w sieci. Korzystanie z serwera Exchange nie jest konieczne, ponieważ system macOS współdziała także z innymi serwerami obsługującymi standardy branżowe, np. IMAP, POP, SMTP, CalDAV, CardDAV czy LDAP. Konieczne jest przetestowanie podstawowych procedur obsługi poczty e-mail, kontaktów i kalendarzy, jak również innego korporacyjnego oprogramowania biurowego i wspomagającego pracę grupową, które stosowane jest przez użytkowników w największym odsetku ich codziennych procedur.

Więcej informacji o konfigurowaniu serwera Microsoft Exchange:
support.apple.com/guide/deployment-reference-macos

Więcej informacji o usługach bazujących na standardach:
support.apple.com/guide/deployment-reference-macos

Magazyn zawartości

Wbudowana w system macOS usługa magazynowania przechowuje lokalnie treści często pobierane z serwerów Apple, minimalizując tym samym obciążenie łącza internetowego przez użytkowników pozyskujących te materiały w sieci firmowej. Magazyn zawartości można wykorzystać do przyspieszenia pobierania i dostarczania oprogramowania za pośrednictwem Mac App Store. Usługa może również magazynować uaktualnienia oprogramowania, aby przyspieszyć pobieranie ich na urządzenia z systemami macOS, iOS lub iPadOS funkcjonujące w organizacji. Korzystając z rozwiązań innych firm, np. Cisco lub Akamai, można magazynować również inne treści.

Więcej informacji o magazynie zawartości:
support.apple.com/guide/deployment-reference-macos

Wybór i wdrożenie rozwiązania do zarządzania

Rozwiązania MDM umożliwiają bezpieczne rejestrowanie komputerów Mac w środowisku biznesowym, bezprzewodowe konfigurowanie i modyfikowanie ustawień, instalowanie aplikacji, monitorowanie przestrzegania zasad, odpytywanie zarządzanych urządzeń oraz ich zdalne wymazywanie lub blokowanie. Zespół IT może w prosty sposób tworzyć profile wykorzystywane w zarządzaniu kontami użytkowników, konfigurowaniu ustawień systemowych, egzekwowaniu ograniczeń i definiowaniu zasad dotyczących haseł — a wszystkie te działania dostępne są w ramach tego samego rozwiązania MDM, które obecnie obsługuje iPhone'y i iPady.

Za kulisami wszystkie platformy Apple korzystają z tej samej architektury zarządzania opracowanej przez Apple i umożliwiającej klientom pracę z różnymi rozwiązaniami MDM innych firm. Na rynku istnieje cała gama rozwiązań do zarządzania urządzeniami, oferowanych przez takie firmy, jak Jamf, VMware i MobileIron. Mimo że wiele architektur używanych do zarządzania urządzeniami w systemie macOS to te same architektury, które występują w systemach iOS i iPadOS, rozwiązania MDM innych firm różnią się nieznacznie pod względem funkcji administracyjnych, obsługi systemów operacyjnych, struktury cen i modelu utrzymywania serwera. Różnice mogą także dotyczyć poziomu oferowanych usług integracyjnych, szkoleniowych oraz wsparcia. Wybór rozwiązania powinien być poprzedzony analizą istotności funkcji w konkretnej organizacji.

Po wybraniu rozwiązania MDM trzeba będzie odwiedzić portal Apple Push Certificates Portal i zalogować się w celu utworzenia nowego certyfikatu dla aktywnej komunikacji MDM.

Więcej informacji o wdrażaniu rozwiązania MDM:
support.apple.com/guide/deployment-reference-macos

Apple Push Certificates Portal:
identity.apple.com/pushcert/

Rejestracja w usłudze Apple Business Manager

Apple Business Manager to portal WWW przeznaczony dla administratorów IT, który umożliwia wdrażanie urządzeń iPhone, iPad, iPod touch, Apple TV i Mac w sposób scentralizowany — z jednego miejsca. Dzięki bezproblemowej współpracy z systemem zarządzania urządzeniami mobilnymi (Mobile Device Management, MDM) używanym w tej samej firmie lub instytucji, Apple Business Manager ułatwia automatyzację wdrażania urządzeń, kupowanie aplikacji, dystrybucję treści i tworzenie zarządzanych kont Apple ID dla pracowników.

Program rejestracji urządzeń (Device Enrollment Program, DEP) i program zakupów grupowych (Volume Purchase Program, VPP) zostały włączone do portalu Apple Business Manager, zatem wszystkie funkcje potrzebne organizacji do wdrażania urządzeń Apple są dostępne w jednym miejscu. Począwszy od 1 grudnia 2019 roku programy te nie będą już dostępne.

Urządzenia

Apple Business Manager umożliwia zautomatyzowaną rejestrację urządzeń, udostępniając szybką, sprawną metodę wdrażania urządzeń Apple należących do firmy oraz rejestracji w systemie MDM bez fizycznej interakcji z urządzeniami i bez konieczności ich przygotowywania.

- Poprzez usprawnienie wykonania odpowiednich kroków w Asystencie ustawień możliwe jest uproszczenie procesu konfiguracji z perspektywy użytkownika, tak by pracownicy dysponowali właściwie skonfigurowanym urządzeniem od razu po aktywacji. Zespoły IT mogą teraz w szerszym zakresie adaptować proces konfiguracji, przez który przechodzą pracownicy, wprowadzając do niego tekst zgody, elementy marki firmy lub nowoczesne mechanizmy uwierzytelniania.

- Nadzór — czyli dodatkowe mechanizmy niedostępne w innych modelach wdrożenia, takie jak niewyłączalne zarządzanie MDM — zapewnia wyższy poziom kontroli nad urządzeniami należącymi do firmy.
- Zarządzanie domyślnymi serwerami MDM jest łatwiejsze, ponieważ można przyporządkować je do określonych rodzajów urządzeń. Za pomocą aplikacji Apple Configurator 2 można także ręcznie rejestrować urządzenia iPhone, iPad i Apple TV niezależnie od tego, w jaki sposób zostały nabyte.

Treści

Apple Business Manager umożliwia organizacjom łatwe hurtowe kupowanie treści. Niezależnie od tego, czy pracownicy używają iPhone'ów, iPadów czy Maców, można w elastyczny i bezpieczny sposób udostępniać im atrakcyjne treści od razu gotowe do wykorzystania.

- Aplikacje, książki i aplikacje niestandardowe — w tym opracowane wewnętrznie przez organizację — można kupować hurtowo. Przenoszenie licencji na aplikacje między lokalizacjami i współużytkowanie licencji przez różnych nabywców z tej samej lokalizacji nie sprawia żadnych trudności. Oprócz tego dostępna jest ogólna lista historii zakupów zawierająca informacje o liczbie licencji aktualnie użytkowanych za pośrednictwem rozwiązania MDM.
- Aplikacje i książki można dystrybuować bezpośrednio do zarządzanych urządzeń lub autoryzowanych użytkowników i bez trudu sprawdzać, jakie treści zostały przydzielone do danego użytkownika lub urządzenia. Dzięki zarządzanej dystrybucji można sprawować kontrolę nad całym procesem udostępniania, zachowując przy tym pełną własność aplikacji. Gdy aplikacja przestanie być potrzebna użytkownikowi lub na urządzeniu, można cofnąć uprawnienia do korzystania z niej i przekazać je innemu użytkownikowi lub przenieść na inne urządzenie w organizacji.
- Zakupu można dokonać za pomocą różnych metod płatności, na przykład przy użyciu karty kredytowej lub na podstawie zamówienia. Organizacje mogą również kupować środki w programie na zakupy hurtowe (tam, gdzie opcja ta jest oferowana) — bezpośrednio od Apple lub od sprzedawców Apple Authorized Reseller — o określonych kwotach wyrażonych w walucie lokalnej, które są następnie elektronicznie wysyłane właścicielowi konta w formie środków na zakupy.
- Dystrybucję aplikacji można prowadzić w wielu krajach, udostępniając je urządzeniom i użytkownikom we wszystkich państwach, w których te aplikacje są dostępne. Deweloperzy mogą udostępniać swoje aplikacje w wielu krajach w ramach standardowego procesu publikowania w App Store.

Uwaga: W niektórych krajach lub regionach zakup książek w portalu Apple Business Manager nie jest możliwy. Informacje o tym, gdzie poszczególne funkcje i metody zakupu są dostępne, znajdują się na stronie support.apple.com/HT207305.

Użytkownicy

Apple Business Manager umożliwia organizacjom tworzenie dla pracowników kont zintegrowanych z istniejącą już infrastrukturą, które pozwalają na dostęp do aplikacji i usług Apple oraz do samego portalu Apple Business Manager, a także zarządzanie tymi kontami.

- Zarządzane konta Apple ID utworzone dla pracowników służą im do zespołowej pracy z wykorzystaniem aplikacji i usług Apple, a także dają dostęp do danych związanych z pracą w aplikacjach zarządzanych korzystających z iCloud Drive. Każda organizacja jest właścicielem takich kont i sprawuje nad nimi kontrolę.
- Połączenie portalu Apple Business Manager z usługą Microsoft Azure Active Directory otwiera drogę do uwierzytelniania federacyjnego. Zarządzane konto Apple ID dla pracownika tworzone będzie automatycznie, gdy tylko zaloguje się on po raz pierwszy, używając swoich dotychczasowych danych uwierzytelniających, na zgodnym urządzeniu Apple.

- Nowa funkcja Rejestracja użytkownika w systemach iOS 13, iPadOS i macOS Catalina pozwala na korzystanie z zarządzanych kont Apple ID równolegle z prywatnymi kontami Apple ID na prywatnych urządzeniach pracowników. Alternatywnym modelem jest używanie zarządzanych kont Apple ID na dowolnym urządzeniu jako głównych (i jedynych) kont Apple ID. Zarządzane konta Apple ID dają także dostęp do iCloud w sieci WWW po pierwszym zalogowaniu na urządzeniu Apple.
- Aby efektywnie zarządzać urządzeniami, aplikacjami i kontami w portalu Apple Business Manager, warto przydzielić członkom zespołów IT odpowiednie inne role. Rola Administratora pozwala na zaakceptowanie, w razie potrzeby, formalnych warunków i zasad oraz łatwe przeniesienie odpowiedzialności w wypadku, gdy ktoś opuści organizację.

Uwaga: Funkcja Rejestracja użytkownika nie obsługuje obecnie iCloud Drive. iCloud Drive można używać z zarządzanym kontem Apple ID tylko wtedy, gdy jest to jedyne konto Apple ID na urządzeniu.

Więcej informacji o usłudze Apple Business Manager: apple.com/pl/business/it

Rejestracja w programie Apple Developer Enterprise Program

Program Apple Developer Enterprise Program oferuje kompletny zestaw narzędzi do tworzenia i testowania aplikacji oraz przekazywania ich użytkownikom. Aplikacje mogą być udostępniane na serwerze WWW lub za pomocą rozwiązania MDM. Aplikacje i programy instalacyjne na Maca mogą być podpisywane i poświadczane identyfikatorem dewelopera rozpoznawanym przez funkcję Gatekeeper, która chroni system macOS przed złośliwym oprogramowaniem.

Więcej informacji o programie Developer Enterprise Program: developer.apple.com/programs/enterprise

2. Konfiguracja

Kolejny etap to określenie firmowych zasad i dopilnowanie, aby system zarządzania urządzeniami mobilnymi był odpowiednio przygotowany do skonfigurowania Maców dla pracowników.

Bezpieczeństwo w systemie macOS

Bezpieczeństwo i prywatność to dwa fundamentalne aspekty uwzględniane przy projektowaniu sprzętu, oprogramowania i usług Apple. Chronimy prywatność klientów, stosując silne szyfrowanie i rygorystyczne zasady postępowania ze wszystkimi danymi. Bezpieczna platforma informatyczna dla urządzeń Apple musi obejmować:

- metody zapobiegania używaniu urządzeń przez osoby nieuprawnione i niezgodnie z uprawnieniami;
- ochronę przechowywanych danych, nawet w razie zgubienia lub kradzieży urządzenia;
- protokoły sieciowe i szyfrowanie danych podczas transmisji;
- środki umożliwiające bezpieczne działanie aplikacji, tak by nie zagrażały one integralności platformy.

Wszystkie urządzenia Apple zawierają wielowarstwową strukturę zabezpieczeń, dzięki której mogą bezpiecznie korzystać z usług sieciowych i chronić ważne dane. Do mechanizmów bezpieczeństwa stosowanych w systemach macOS, iOS i iPadOS należy też ochrona za pomocą kodu dostępu oraz zasady stosowania haseł, które mogą być wprowadzane i egzekwowane za pomocą rozwiązania MDM. Jeśli urządzenie wpadnie w niepowołane ręce, użytkownik lub administrator może zdalnie wydać polecenie usunięcia wszystkich poufnych informacji.

Dział IT może za pośrednictwem rozwiązania MDM wprowadzać różne zasady podnoszące poziom bezpieczeństwa urządzeń. Jako przykłady można wskazać egzekwowanie użycia funkcji FileVault i przechowywania klucza odzyskiwania w systemie MDM, wymuszanie określonych zasad dotyczących haseł lub blokowania ekranu przez wygaszacz, a także włączanie wbudowanej zapory.

Więcej informacji o zabezpieczeniach platform Apple: apple.com/security/

Określenie zasad firmowych

Opracowywanie zasad firmowych należy rozpocząć od tych, które dotyczyć będą większości użytkowników komputerów Mac w przedsiębiorstwie. Rozwiązanie MDM umożliwi definiowanie modyfikacji właściwych dla konkretnych użytkowników, np. kont lub uprawnień dostępu do określonych aplikacji. Możliwe jest także określanie zasad obowiązujących w odniesieniu do jednostek organizacyjnych lub innych mniejszych podzbiorów użytkowników, np. wdrażanie określonego oprogramowania lub ustawień używanych tylko w jednym dziale.

We współpracy z odpowiednimi zespołami wewnętrznymi należy zmodyfikować istniejące zasady firmowe, tak aby uwzględniały korzystanie z komputerów Mac. Niektóre podstawowe zasady — takie jak wymagania co do złożoności i rotacji haseł, limity czasu wygaszacza ekranu i reguły dopuszczalnego użycia — są takie same na wszystkich platformach.

Jeśli z obowiązujących w firmie zasad wynika obowiązek korzystania z określonego rozwiązania technicznego obecnego na innej platformie, konieczne jest przeanalizowanie istoty problemu i takie przeformułowanie zasad, by uwzględniały rozwiązania wbudowane w system macOS. Zamiast narzucać wymóg szyfrowania całych dysków za pomocą konkretnego rozwiązania innej firmy, warto rozważyć wprowadzenie ogólnej zasady szyfrowania przechowywanych danych. Użycie funkcji FileVault spełni tak sformułowany wymóg. Jeśli obowiązujące zasady nakazują ochronę przed złośliwym oprogramowaniem przy użyciu wyraźnie wskazanego produktu, należy zapoznać zespoły z wbudowanymi zabezpieczeniami, takimi jak Gatekeeper, a następnie zmodyfikować zasadę, tak aby dopuszczała korzystanie z nich.

Konfiguracja ustawień w rozwiązaniu MDM

Aby umożliwić zarządzanie zasadami firmowymi i zapewnić pracownikom dostęp do niezbędnych zasobów, każdy Mac zostanie w bezpieczny sposób zarejestrowany w wybranym dla firmy rozwiązaniu MDM. Następnie rozwiązanie MDM będzie wprowadzać zasady i ustawienia na podstawie profili konfiguracji. Profile konfiguracji to wygenerowane przez rozwiązanie MDM pliki XML, które umożliwiają dystrybuowanie ustawień do urządzeń. Profile te automatyzują wprowadzanie ustawień i zasad, konfigurowanie kont, ograniczeń i poświadczeń. Mogą być podpisywane i szyfrowane w celu dodatkowego zabezpieczenia systemów organizacji.

Po rejestracji danego urządzenia w rozwiązaniu MDM administrator może wprowadzić za pośrednictwem systemu MDM zasady, a także wysłać zapytanie lub polecenie. Wówczas usługa powiadomień w trybie push firmy Apple (APNs) przez sieć wysyła do urządzenia instrukcję nakazującą bezpośrednie — przy użyciu zabezpieczonego połączenia — komunikowanie się z rozwiązaniem MDM w celu wykonania czynności wskazanej przez administratora. Ponieważ w komunikacji uczestniczy tylko rozwiązanie MDM i urządzenie, usługa APNs nie przesyła informacji poufnych ani zastrzeżonych. Jeśli urządzenie zostanie wyłączone spod zarządzania, ustawienia i zasady, którymi steruje profil konfiguracji, zostaną usunięte. W razie potrzeby firma może także zdalnie wymazać zawartość urządzenia.

W wielu organizacjach rozwiązanie MDM działa w połączeniu z używanymi dotychczas usługami katalogowymi. Podczas zautomatyzowanej rejestracji urządzenia Asystent ustawień w systemie macOS może monitować użytkownika o zalogowanie się przy użyciu danych uwierzytelniających z usługi katalogowej. Nowe opcje konfiguracji rejestracji dostępne w systemie macOS Catalina umożliwiają wyświetlanie interfejsów uwierzytelniania chmurowych dostawców tożsamości w Asystencie ustawień. Gdy urządzenie zostanie przypisane do konkretnego użytkownika, rozwiązanie MDM może dostosować ustawienia konfiguracji i konta do wymagań tej osoby lub grupy. Użytkownik może na przykład automatycznie uzyskać dostęp do swojego konta Microsoft Exchange podczas rejestracji w systemie. Możliwe jest także korzystanie z tożsamości powiązanych z certyfikatami na potrzeby takich rozwiązań, jak na przykład 802.1x lub VPN.

Zważywszy na wysoką skuteczność kontroli, jaką zapewniają te systemy, firmy często bez obaw nadają użytkownikowi uprawnienia administracyjne do Maca. Pozwalają w ten sposób na pełną personalizację ustawień, instalowanie aplikacji i rozwiązywanie ewentualnych problemów, podczas gdy obowiązujące w firmie zasady wciąż są egzekwowane przez rozwiązanie MDM. Z perspektywy użytkownika jest to model uprawnień i mechanizmów kontroli analogiczny do tego, jakim objęte są zarządzane urządzenia iPhone i iPad.

Więcej informacji o profilach konfiguracji:
support.apple.com/guide/deployment-reference-macos

Przygotowanie do zautomatyzowanej rejestracji urządzeń

Najłatwiejszą metodą zautomatyzowanej rejestracji urządzenia w rozwiązaniu MDM jest skorzystanie z funkcji rejestracji urządzeń dostępnych w portalu Apple Business Manager na jednym z etapów działania Asystenta ustawień. Taka rejestracja odbywa się bez interakcji z działem IT i może usprawnić przechodzenie przez niektóre ekrany Asystenta ustawień, zatem cały proces jest szybszy z punktu widzenia użytkownika.

Aby skonfigurować zautomatyzowaną rejestrację urządzeń, należy połączyć rozwiązanie MDM organizacji z jej kontem w usłudze Apple Business Manager za pośrednictwem bezpiecznego tokenu. Proces dwuetapowej weryfikacji bezpiecznie autoryzuje rozwiązanie MDM. Szczegółowych informacji na temat wdrożenia konkretnego rozwiązania MDM może udzielić jego dostawca.

Jeśli urządzenie jest już używane przez pracownika lub jest jego własnością, użytkownik może w Preferencjach systemowych otworzyć jeden profil konfiguracji i zweryfikować go, aby dokończyć rejestrację. Mechanizm ten nazywany jest rejestracją w rozwiązaniu MDM zatwierdzoną przez użytkownika. Rejestracja w ramach procesu rejestracji urządzeń albo rejestracja w rozwiązaniu MDM zatwierdzona przez użytkownika jest niezbędna, aby możliwe było zarządzanie niektórymi ustawieniami istotnymi dla bezpieczeństwa — takimi jak zasady rozszerzeń jądra lub kontrola preferencji zasad prywatności.

Więcej informacji o ładowaniu rozszerzeń jądra:
support.apple.com/guide/deployment-reference-macos

Więcej informacji o kontroli preferencji zasad prywatności:
support.apple.com/guide/mdm

Przygotowanie do dystrybuowania aplikacji i książek

Apple oferuje szeroko zakrojone programy wspierające organizacje w skutecznym wykorzystywaniu fantastycznych aplikacji oraz treści dostępnych na platformie macOS. Mechanizmy te umożliwiają dystrybuowanie wśród pracowników potrzebnych im aplikacji i książek zakupionych za pośrednictwem usługi Apple Business Manager, a także aplikacji stworzonych do wewnętrznego użytku firmy. Rozwiązanie MDM może także dystrybuować aplikacje oraz instalować pakiety oprogramowania niedostępnego w Mac App Store.

Rozwiązanie MDM może korzystać z mechanizmu dystrybucji zarządzanej w odniesieniu do aplikacji i książek zakupionych za pośrednictwem usługi Apple Business Manager w dowolnym kraju, w którym dana aplikacja jest dostępna. Aby korzystać z dystrybucji zarządzanej, należy najpierw połączyć rozwiązanie MDM z kontem w usłudze Apple Business Manager za pomocą bezpiecznego tokenu. Gdy serwer MDM jest już połączony z usługą, zakupione w niej aplikacje i książki można przypisywać do użytkowników, nawet jeśli na ich urządzeniach zablokowana jest obsługa App Store. Można także przypisywać aplikacje bezpośrednio do urządzeń, co istotnie ułatwia wdrożenie, ponieważ umożliwia korzystanie z aplikacji każdemu użytkownikowi mającemu dostęp do tego urządzenia.

Więcej informacji o kupowaniu treści w usłudze Apple Business Manager:
support.apple.com/guide/apple-business-manager

Więcej informacji o dystrybucji aplikacji i książek:
support.apple.com/guide/apple-business-manager

Przygotowanie dodatkowych treści

Rozwiązanie MDM może pomóc w dystrybucji dodatkowych pakietów treści niepochodzących z Mac App Store. Takie podejście jest często stosowane w odniesieniu do oprogramowania klasy korporacyjnej, np. własnych aplikacji na użytek wewnętrzny albo takich aplikacji, jak Chrome lub Firefox. Wymagane oprogramowanie może być tą metodą aktywnie rozsyłane do urządzeń i automatycznie instalowane po zakończeniu rejestracji. Również czcionki, skrypty i inne elementy można instalować i wykonywać za pośrednictwem pakietów. Należy zadbać o to, aby te pakiety były odpowiednio podpisane za pomocą ID dewelopera z programu Developer Enterprise Program.

Więcej informacji o instalowaniu dodatkowych treści:
support.apple.com/guide/deployment-reference-macos

3. Wdrożenie

System macOS oferuje mechanizmy, które umożliwiają łatwe wdrożenie i personalizację urządzeń przeznaczonych dla użytkowników. Wszystko odbywa się bez angażowania działu IT, a pracownicy mogą od razu przystąpić do pracy z nowym systemem.

Zastosowanie Asystenta ustawień

Na samym początku pracownicy mogą wybrać za pomocą Asystenta ustawień w systemie macOS preferowany język i region oraz połączyć się z siecią. Po połączeniu się z Internetem użytkownicy zobaczą szereg okien Asystenta ustawień, które poprowadzą ich krok po kroku przez wstępną konfigurację nowego Maca. W ramach tego procesu urządzenia zarejestrowane w usłudze Apple Business Manager mogą zostać automatycznie zarejestrowane także w rozwiązaniu MDM. Systemy Mac zarejestrowane jako urządzenia można skonfigurować tak, aby pomijały wybrane ekrany, na przykład stronę z warunkami programu, stronę logowania się na koncie Apple ID, okna usług lokalizacji i inne.

Po Asystencie ustawień do akcji może wkroczyć rozwiązanie MDM, które w ramach początkowej konfiguracji wdroży różne ustawienia, m.in. określi, czy użytkownik będzie miał pełne uprawnienia administracyjne na swoim komputerze. Podobnie jak w przypadku iPhone'ów i iPadów, takie rozwiązanie zapewnia użytkownikowi kontrolę nad urządzeniem, a jednocześnie wymusza przestrzeganie firmowych zasad i stosowanie ustawień podlegających zarządzaniu MDM. Aby użytkownik mógł przystąpić do pracy od razu po zakończeniu działania Asystenta ustawień, automatycznie zainicjowany proces pobierania i instalowania w tle powinien obejmować tylko najważniejsze, niezbędne aplikacje i pakiety. Użytkownik może samodzielnie ustalić późniejszy termin pobrania i instalacji (w tle) większych aplikacji, korzystając z narzędzia samoobsługowego wchodzącego w skład rozwiązania MDM.

Konfigurowanie kont firmowych

MDM może automatycznie skonfigurować konto pocztowe i inne konta użytkownika. W zależności od używanego rozwiązania MDM i integracji z systemami wewnętrznymi przypisane do konta pakiety mogą już wstępnie zostać uzupełnione o nazwę użytkownika i jego adres e-mail, a także o tożsamości certyfikatów do uwierzytelniania i podpisywania.

Personalizacja przez użytkowników

Umożliwienie użytkownikom personalizacji urządzeń sprzyja produktywności pracy, ponieważ pracownicy mogą wówczas sami wybrać aplikacje i treści, które najskuteczniej pomogą im w realizacji indywidualnych zadań oraz celów. Zarządzane konta Apple ID i funkcja Rejestracja użytkownika w systemie macOS Catalina stwarzają organizacjom nowe możliwości zapewnienia użytkownikom dostępu do usług Apple z firmowych kont Apple ID — wyłącznie z nich albo równolegle z osobistymi kontami Apple ID.

Konta Apple ID i zarządzane konta Apple ID

Gdy pracownik loguje się na swoim koncie Apple ID w usługach Apple, takich jak FaceTime, iMessage, App Store czy iCloud, uzyskuje dostęp do szerokiej gamy treści ułatwiających sprawne wykonywanie zadań zawodowych oraz sprzyjających wysokiej wydajności oraz pracy zespołowej. Tak jak wszystkie konta Apple ID, zarządzane konta Apple ID służą do logowania się na osobistym urządzeniu. Zapewniają także dostęp do usług Apple — w tym iCloud i funkcji pracy zespołowej w aplikacjach iWork i Notatki — oraz do portalu Apple Business Manager. W odróżnieniu od zwykłych kont Apple ID, zarządzane konta Apple ID są własnością poszczególnych organizacji i są przez nie zarządzane — dotyczy to m.in. resetowania haseł i administrowania na podstawie ról. Niektóre ustawienia zarządzanych kont Apple ID podlegają ograniczeniom.

Urządzenia rejestrowane za pomocą funkcji Rejestracja użytkownika wymagają zarządzanych kont Apple ID. Rejestracja użytkownika obsługuje opcjonalne osobiste konta Apple ID; pozostałe opcje rejestracji pozwalają na stosowanie albo osobistego, albo zarządzanego konta Apple ID. Tylko funkcja Rejestracja użytkownika obsługuje więcej niż jedno konto Apple ID.

Aby jak najefektywniej korzystać z tych usług, użytkownicy powinni używać własnych kont Apple ID lub założonych dla nich zarządzanych kont Apple ID. Użytkownik bez konta Apple ID może je utworzyć jeszcze przed otrzymaniem urządzenia. Jeśli użytkownik nie ma jeszcze osobistego konta Apple ID, to może je utworzyć w Asystencie ustawień. Do założenie konta Apple ID nie jest potrzebna karta kredytowa.

Więcej informacji o zarządzanych kontach Apple ID:
support.apple.com/guide/deployment-reference-macos

iCloud

iCloud automatycznie synchronizuje i uaktualnia dokumenty oraz prywatne treści użytkowników — takie jak kontakty, kalendarze, pliki tekstowe i zdjęcia — na wielu urządzeniach jednocześnie. Funkcja Znajdź mój umożliwia użytkownikowi odszukanie zgubionego lub skradzionego Maca, iPhone'a, iPada lub iPoda touch. Wybrane funkcje iCloud — takie jak Pęk kluczy iCloud i iCloud Drive — można wyłączyć poprzez nałożenie ograniczeń wprowadzonych ręcznie na urządzeniu lub za pośrednictwem rozwiązania MDM. Dzięki temu organizacja ma większy wpływ na to, jakie dane są przechowywane na poszczególnych kontach.

Więcej informacji o zarządzaniu usługami iCloud:
support.apple.com/guide/deployment-reference-macos

4. Zarządzanie

Po przygotowaniu i uruchomieniu urządzeń organizacja ma do dyspozycji wiele funkcji administracyjnych, które umożliwiają ciągłe zarządzanie urządzeniami i treścią, a także ich kontrolę.

Administrowanie urządzeniami

Rozwiązania MDM mogą administrować zarządzanymi urządzeniami, realizując szereg zadań. Należy do nich wysyłanie do urządzeń zapytań, a także inicjowanie czynności, dzięki którym można kontrolować urządzenia, które zostały zagubione bądź skradzione lub są wykorzystywane niezgodnie z polityką firmy.

Zapytania

Rozwiązanie MDM może wysyłać do urządzeń zapytania o różne informacje, aby sprawdzać, czy są na nich zainstalowane odpowiednie aplikacje i wybrane właściwe ustawienia. Pytania mogą dotyczyć sprzętu, np. numeru seryjnego lub modelu urządzenia, albo oprogramowania, np. wersji systemu macOS lub listy zainstalowanych aplikacji. Ponadto rozwiązanie MDM może pytać o stan najważniejszych funkcji zabezpieczających, takich jak FileVault lub wbudowana zapora.

Zadania administracyjne

Rozwiązanie MDM może wykonywać szereg różnych zadań administracyjnych na zarządzanych urządzeniach, m.in. automatycznie zmieniać ustawienia konfiguracyjne bez interakcji z użytkownikiem, uaktualniać system macOS, zdalnie blokować urządzenia lub wymazywać ich zawartość oraz zarządzać hasłami.

Więcej informacji o zadaniach administracyjnych:
support.apple.com/guide/deployment-reference-macos

Zarządzanie uaktualnieniami oprogramowania

Dział IT może zapewnić użytkownikom możliwość uaktualnienia systemu operacyjnego do najnowszej wersji, gdy tylko stanie się ona dostępna. Testując wersję wstępną macOS, informatycy mają okazję zawczasu zidentyfikować problemy z kompatybilnością aplikacji i zgłosić je programistom przed premierą ostatecznej wersji systemu. Dział IT może brać udział w testowaniu każdej nowej wersji systemu w ramach programu Apple Beta Software Program lub AppleSeed for IT. Ze względu na bezpieczeństwo użytkowników i ich danych ważne jest wdrożenie kompleksowej strategii uaktualniania komputerów Mac. Należy regularnie i często instalować uaktualnienia, a nowe główne wydania systemu macOS wdrażać od razu po potwierdzeniu ich zgodności z obowiązującymi procedurami i metodami pracy.

Rozwiązanie MDM może automatycznie, aktywnie przekazywać uaktualnienia systemu macOS do komputerów Mac zarejestrowanych jako urządzenia. Maca zarejestrowanego jako urządzenie można też skonfigurować w taki sposób, aby uaktualnienia i powiadomienia o uaktualnieniach były odłożone w czasie o maksymalnie 90 dni — jeśli newralgiczne systemy firmy nie są jeszcze gotowe na nową wersję oprogramowania. Na tak skonfigurowanym Macu użytkownik nie będzie mógł ręcznie inicjować uaktualnień, dopóki odpowiednia zasada nie zostanie usunięta lub rozwiązanie MDM nie wyśle polecenia instalacji.

Firma Apple nie zaleca uaktualniania systemu macOS w postaci monolitycznych obrazów systemu ani nie zapewnia wsparcia dla takiego rozwiązania. Na komputerach Mac, podobnie jak na urządzeniach iPhone i iPad, często instalowane są uaktualnienia oprogramowania sprzętowego właściwe dla konkretnego modelu. Z kolei uaktualnienia systemu operacyjnego dla Maca wymagają zainstalowania tych uaktualnień oprogramowania sprzętowego bezpośrednio od Apple. Najbardziej niezawodną strategią jest użycie do uaktualnienia Instalatora systemu macOS lub poleceń systemu MDM.

Zarządzanie dodatkowym oprogramowaniem

Często pojawia się potrzeba dostarczenia użytkownikom dodatkowych aplikacji spoza pierwotnie instalowanego zestawu. Rozwiązanie MDM może wykonywać to zadanie automatycznie w odniesieniu do newralgicznych aplikacji i uaktualnień. Możliwy jest także model zaopatrzenia w oprogramowanie „na żądanie", w którym pracownicy zamawiają aplikacje w samoobsługowym portalu rozwiązania MDM. Takie portale oferują szerokie spektrum możliwości, od instalacji oprogramowania kupionego w App Store za pośrednictwem usługi Apple Business Manager po obsługę aplikacji, skryptów i innych narzędzi spoza App Store.

Większość oprogramowania można instalować automatycznie, jednak niektóre instalacje mogą wymagać interakcji z użytkownikiem. Ze względów bezpieczeństwa aplikacje, które wymagają rozszerzeń jądra, ładowane są obecnie dopiero wtedy, gdy użytkownik wyrazi na to zgodę. Mechanizm ten nazywany jest zatwierdzaniem przez użytkownika wczytywania rozszerzeń jądra i może podlegać zarządzaniu MDM.

Nadzór nad bezpieczeństwem urządzeń

Przed wdrożeniem urządzeń organizacja przyjęła wstępny zestaw zasad bezpieczeństwa. Ich faktyczne przestrzeganie musi być jednak monitorowane, a odpowiedzialny za to zespół będzie prawdopodobnie chciał maksymalnie wykorzystać w tym celu funkcje raportowania, jakie oferuje rozwiązanie MDM. Raporty mogą dotyczyć ogólnego stanu zabezpieczeń na każdym urządzeniu lub służyć do zbierania danych o instalacji poprawek oprogramowania. Mimo że dla większości organizacji wystarczające są natywne narzędzia do szyfrowania i ochrony Maca, w niektórych instytucjach i firmach obowiązkowe jest stosowanie dodatkowych usług synchronizacji i udostępniania plików lub narzędzi zapobiegających utracie danych, które chronią przed wyciekami informacji i generują pogłębione raporty o stanie danych wrażliwych.

Funkcja Znajdź mój Mac usługi iCloud umożliwia zdalne zainicjowanie wymazywania zgubionego lub skradzionego Maca, czyli jego dezaktywację po uprzednim usunięciu z niego wszystkich danych. Zespoły IT mogą również zdalnie inicjować wymazywanie za pośrednictwem rozwiązania MDM.

Przekazywanie urządzeń innym użytkownikom

Gdy pracownik odejdzie z organizacji, jego Maca można łatwo przygotować do przekazania innemu użytkownikowi, korzystając z funkcji odzyskiwania systemu przez Internet i lokalnej partycji odzyskiwania. Zawartość Maca jest wymazywana, a na komputerze instalowana jest najnowsza wersja systemu operacyjnego. Mac przypisany do konkretnego rozwiązania MDM w usłudze Apple Business Manager automatycznie z powrotem zarejestruje się w tym rozwiązaniu podczas konfiguracji w Asystencie ustawień, skonfiguruje ustawienia dla nowego użytkownika, zastosuje zasady firmowe i zainstaluje odpowiedni zestaw oprogramowania. Niezarejestrowane komputery Mac można w ten sam sposób wymazać i przygotować dla nowego użytkownika, a potem ręcznie zarejestrować w rozwiązaniu MDM.

Opcje wsparcia

Wiele organizacji przekonuje się, że użytkownicy komputerów Mac korzystają z pomocy informatyków w minimalnym stopniu. Aby zachęcić pracowników do samodzielnego rozwiązywania problemów oraz im to ułatwić, większość działów IT opracowuje narzędzia do samopomocy technicznej. Mogą to być na przykład: strona internetowa oferująca kompleksowe wsparcie dla komputera Mac, fora internetowe poświęcone samopomocy lub znajdujące się bezpośrednio w placówce organizacji punkty pomocy technicznej. Rozwiązania MDM mogą też udostępniać użytkownikom funkcje należące do obszaru wsparcia technicznego, np. instalowanie lub uaktualnianie oprogramowania z portalu samoobsługowego.

Do dobrych praktyk należy mieszane podejście do wsparcia dla użytkowników. Jego istotą jest promowanie zespołowego rozwiązywania problemów i stworzenie warunków do samopomocy. Użytkownicy kontaktują się z działem wsparcia dopiero wtedy, gdy nie uda im się samodzielnie pokonać trudności. Warto zachęcać użytkowników do zaangażowania w ten proces i pewnej autonomii w poszukiwaniu rozwiązań.

Współodpowiedzialność za wsparcie techniczne przyczynia się do skrócenia przerw w pracy i obniżenia łącznych kosztów osobowych i kosztów zapewnienia wsparcia. Organizacjom, którym to nie wystarcza, plan AppleCare zapewnia różnorodne usługi i programy uzupełniające wewnętrzne struktury wsparcia dla pracowników i działu IT.

AppleCare for Enterprise

Firmy zainteresowane pełną ochroną mogą przystąpić do planu AppleCare dla przedsiębiorstw, który pozwala im odciążyć wewnętrzne centrum pomocy, zapewniając telefoniczne, całodobowe wsparcie techniczne dla pracowników i jednogodzinny czas reakcji w wypadku najpoważniejszych problemów. Program ten obejmuje również adresowane do działów IT wsparcie w realizacji scenariuszy integracji, w tym także w wypadku rozwiązań MDM i Active Directory.

AppleCare OS Support

W ramach usługi AppleCare OS Support działom IT zapewniane jest telefoniczne i elektroniczne wsparcie na poziomie korporacyjnym dotyczące wdrażania systemów iOS, iPadOS, macOS i macOS Server. W zależności od zakresu wykupionej usługi może ona obejmować pomoc 24/7 i wsparcie przypisanego opiekuna technicznego. Oferując możliwość bezpośredniego zadawania pytań o integrację, migrację i problemy z zawansowaną eksploatacją serwerów specjaliście, usługa AppleCare OS Support pozwala zespołom IT efektywniej wdrażać urządzenia i zarządzać nimi, a także sprawniej rozwiązywać problemy.

AppleCare Help Desk Support

Plan AppleCare Help Desk Support umożliwia priorytetowy dostęp telefoniczny do najbardziej doświadczonych pracowników działu wsparcia Apple. Ponadto decydując się na ten plan, organizacja otrzyma pakiet narzędzi wspomagających diagnostykę i rozwiązywanie problemów ze sprzętem Apple, co pozwoli jej efektywniej zarządzać zasobami, skrócić czas reakcji na zgłoszenia i obniżyć koszty przeszkolenia. Plan wsparcia AppleCare Help Desk Support obejmuje nieograniczoną liczbę incydentów związanych z diagnostyką i rozwiązywaniem problemów dotyczących sprzętu i oprogramowania, a także z izolowaniem problemów w urządzeniach z systemami iOS i iPadOS.

AppleCare i AppleCare+ dla Maca

Każdy Mac objęty jest roczną ograniczoną gwarancją oraz 90-dniowym bezpłatnym telefonicznym wsparciem technicznym. Wykupując plan ochrony AppleCare+ lub AppleCare Protection Plan, okres ochrony urządzenia można wydłużyć do trzech lat od pierwotnej daty zakupu urządzenia. W tym czasie pracownicy swoje pytania o sprzęt i oprogramowanie Apple mogą kierować telefonicznie do zespołu Wsparcia Apple. Ponadto Apple zapewnia dostęp do wygodnych form obsługi serwisowej, gdy zajdzie konieczność naprawy urządzenia. Oprócz tego plan AppleCare+ dla Maca obejmuje również naprawę urządzenia w razie jego przypadkowego uszkodzenia w określonych okolicznościach. Za każdą taką naprawę klient jest obciążany opłatą serwisową.

Więcej informacji o opcjach wsparcia AppleCare:
apple.com/support/professional/

Podsumowanie

Niezależnie od tego, czy z komputerów Mac ma korzystać wybrana grupa pracowników, czy cała organizacja, firma ma do dyspozycji wiele rozwiązań upraszczających wdrażanie urządzeń i zarządzanie nimi. Wybór strategii najlepszej dla instytucji może przyczynić się do wzrostu produktywności pracy i sprawić, że pracownicy zaczną bardziej innowacyjnie podchodzić do realizacji swoich obowiązków.

Informacje o funkcjach systemu macOS związanych z wdrażaniem, zarządzaniem i zabezpieczeniami:
support.apple.com/guide/deployment-reference-macos

Informacje o ustawieniach zarządzania urządzeniami mobilnymi przeznaczonych dla zespołów IT:
support.apple.com/guide/mdm

Informacje o usłudze Apple Business Manager:
support.apple.com/guide/apple-business-manager

Informacje o zarządzanych kontach Apple ID dla firm:
apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Informacje o inicjatywie Apple w pracy:
www.apple.com/pl/business/

Informacje o funkcjach przeznaczonych dla zespołów IT:
www.apple.com/pl/business/it/

Informacje o zabezpieczeniach platform Apple:
www.apple.com/security/

Oferta programów AppleCare:
www.apple.com/support/professional/

Szkolenia i certyfikaty Apple:
training.apple.com

Kontakt z działem Apple Professional Services:
consultingservices@apple.com