

# Jak radzić sobie z mobilnym udostępnianiem plików

---

## Komu można zaufać i powierzyć zasoby firmy?

---

Zapewnienie pracownikom mobilnego dostępu do plików i możliwości ich współdzielenia to już nie tylko moda, ale coraz częściej konieczność. Jeżeli nie zapewnisz swoim użytkownikom bezpiecznego, sensownego rozwiązania pozwalającego na pobieranie i udostępnianie plików w podróży, wezmą sprawy w swoje ręce. Na pewno zdajesz sobie sprawę, że najczęściej kończy się to tak, że dane firmowe przechowywane są w chmurze w serwisach przeznaczonych dla konsumentów.. Jeśli to doświadczenie masz już za sobą i szukasz teraz mobilnego rozwiązania dostępu do plików i udostępniania danych, które bardziej sprzyjałoby potrzebom firmy, musisz zdać sobie sprawę, że wiele dostępnych na rynku produktów pozbawionych jest niezbędnych zabezpieczeń, tłumi produktywność użytkowników i przysparza dodatkowej pracy działom informatycznym, które i tak są już obciążone do granic możliwości.

# Ocena różnych klas produktów oferujących mobilny dostęp do plików

Zapewnienie pracownikom mobilnego dostępu do plików i możliwości ich współdzielenia to już nie tylko moda, ale coraz częściej konieczność. Jeżeli nie zapewnisz swoim użytkownikom bezpiecznego, sensownego rozwiązania pozwalającego na pobieranie i udostępnianie plików w podróży, wiedz, że wezmą sprawę w swoje ręce.

---

**Potwierdzają to badania przeprowadzone w czerwcu 2012 r. przez firmę SkyDox. Z łącznej liczby 4000 ankietowanych pracowników 55% przyznało się do udostępniania dokumentów firmy za pośrednictwem bezpłatnych platform oferujących tego rodzaju usługi, z czego 55% zrobiło to bez wiedzy firmowego działu IT.**

Zwiększenie produktywności i oszczędność czasu uzyskane dzięki nieograniczonemu przez czas i miejsce dostępowi do plików są dla użytkowników więcej niż wystarczającą zachętą, by przymknąć oko na zagrożenia związane z umieszczaniem firmowych danych w chmurze w serwisach dla konsumentów. Tych zagrożeń nie mogą jednak zignorować działy informatyczne. Sposób, w jaki użytkownicy mobilni postępują z tymi cennymi zasobami cyfrowymi może budzić przerażenie. Jak zawsze trzeba jednak znaleźć równowagę między wymogami ładu korporacyjnego a potrzebami użytkowników.

Być może zastanawiasz się już nad wyborem mobilnego rozwiązania dostępu do plików i udostępniania danych, które byłoby bardziej odpowiednie dla firmy. Jeśli tak — doskonale. Musisz jednak wiedzieć, że wiele spośród licznych klas rozwiązań, jakie istnieją na rynku, pozbawionych jest niezbędnych zabezpieczeń, tłumi produktywność użytkowników i przysparza dodatkowej pracy działom informatycznym, które i tak są już obciążone do granic możliwości.

## Usługi w chmurze dla konsumentów

Organizacje, które dopuszczają, by ich użytkownicy samodzielnie wybierali rozwiązania mobilnego dostępu do plików odkrywają, że wybierają oni produkty przeznaczone dla zwykłych użytkowników, takie jak Dropbox, Google Drive czy SkyDrive. Rejestracja w tych usługach jest prosta i można szybko zacząć z nich korzystać. Ich głównym zadaniem jest jednak służyć jak największej liczbie osób, a nie dbać o bezpieczeństwo przedsiębiorstwa. Stąd pojawiające się w wiadomościach informacje o lukach w zabezpieczeniach czy przerwach w działaniu.

Oprócz tego, że usługi te są pozbawione mechanizmów uwierzytelniania i zabezpieczeń klasy biznesowej, które funkcjonują już w Twojej firmie, to pozostają one poza zasięgiem twojej kontroli. Masz niewielki lub wręcz żaden wpływ na to, jakie pliki użytkownicy mogą przechowywać w tych serwisach i udostępniać za ich pomocą. Co dzieje się z plikami firmy przechowywanymi na osobistym koncie pracownika w usłudze przechowywania w chmurze, gdy pracownik ten odchodzi lub zostaje zwolniony z firmy? Wszystkie konsumenckie usługi przechowywania w chmurze odbierają ci zdolność do ochrony własności intelektualnej i zapobiegania wyciekom danych. Twoim zadaniem w zakresie rozwiązań informatycznych jest uprzedzić działania użytkowników poprzez dostarczenie im lepszej alternatywy.

## Usługi w chmurze dla przedsiębiorstw

W obliczu braku odpowiednich zabezpieczeń w usługach konsumenckich na rynku pojawiły się inne oparte na chmurze produkty, dążące do wypełnienia powstałej luki i nastawione na spełnienie wymagań przedsiębiorstw. Przyciągały one klientów mechanizmami zabezpieczeń i kontroli klasy korporacyjnej i dawały administratorom IT możliwość zarządzania prawami dostępu i zasadami uwierzytelniania. Rozwiązania oferujące wysokiej klasy zabezpieczenia i mechanizmy kontroli może się podobać, szczególnie w połączeniu z obietnicą uwolnienia od ciężaru hostowania infrastruktury pamięci masowej i zarządzania nią. Mogą nawet wydawać się idealnym wyjściem dla firmy chcącej w bezpieczny sposób wyposażyć swoich użytkowników mobilnych w możliwości dostępu do plików i ich udostępniania. Nie tak szybko. Tak zwane usługi przechowywania w chmurze klasy korporacyjnej mają trzy zasadnicze wady.

## Podwojenie ilości pracy przy zarządzaniu

Pierwszą wadą zastosowania przeznaczonych dla firm usług przechowywania w chmurze do zapewnienia mobilnego dostępu do plików jest podwojenie ilości pracy przy zarządzaniu. Wprowadzenie, a następnie precyzyjne dostrojenie mechanizmów zabezpieczeń i praw dostępu do

---

danych twojej firmy trwale zapewne kilka lat. Oferowane rozwiązania oznaczają ponowne zmierzenie się z tym pracochłonnym procesem, lecz tym razem przy użyciu ich własnych narzędzi zabezpieczeń, a nie tych, które już znasz i do których masz zaufanie. Z chwilą sięgnięcia po nie zyskasz też stałe zajęcie w postaci zarządzania nową infrastrukturą hostowaną, którą trzeba się będzie zająć osobno, równoległe z zarządzaniem infrastrukturą danych w firmie.

### **Puste repozytoria danych**

Drugą wadą opisywanych rozwiązań opartych na chmurze, być może najistotniejszą i często pomijaną w analizach, jest trudność migrowania danych z infrastruktury przedsiębiorstwa do chmury. Trzeba przyjrzeć się temu zagadnieniu i spróbować realistycznie ocenić, ile tygodni czy miesięcy pracy będzie kosztowało przeniesienie wszystkich tych plików do miejsca przechowywania w chmurze. Przeniesiesz je wszystkie? A może część z nich? Czy będzie to całkowite przeniesienie, czy może tylko kopiowanie, które pociągnie za sobą zduplikowanie danych? Jak rozpoznasz pliki, których Twoi użytkownicy będą faktycznie chcieli lub potrzebowali w chmurze?

Zwykle dział IT zostawia tę sprawę użytkownikom. Pod pewnymi względami ma to sens. Przenosząc ciężar decyzji na użytkowników, nie można jednak mieć nawet pewności, że kiedykolwiek skorzystają oni z inwestycji w nową usługę. Gdy do wyboru jest rozwiązanie konsumenckie, gdzie użytkownik ma już zapisane pliki, oraz nowa usługa firmowa, która pozostaje pustym repozytorium, dopóki ktoś nie zajmie się skopiowaniem lub przeniesieniem do niej zawartości, wynik z punktu widzenia zasad i kontroli jest na ogół niekorzystny.

### **Duplikowanie plików i kontrola wersji**

Kopiowanie danych z wewnętrznego repozytorium firmy do hostowanej usługi w chmurze oznacza duże prawdopodobieństwo problemów z duplikatami plików i kontrolą wersji. Użytkownicy mogą nie pamiętać lub wręcz nie wiedzieć, które z plików zostały już przeniesione do chmury. Jednego dnia mogą pracować na wersji zapisanej w chmurze, by tydzień czy dwa później wprowadzać zmiany w wersji zapisanej na korporacyjnym serwerze plików. Taka sytuacja jest jeszcze bardziej prawdopodobna (i potencjalnie bardziej niebezpieczna), gdy użytkownicy współużytkują pliki — różne osoby mogą wtedy pracować na różnych wersjach tego samego dokumentu przechowywanych w różnych repozytoriach. Część tak zwanych usług typu cloud dla przedsiębiorstw obejmuje narzędzia do audytu, umożliwiające rozwiązanie problemu kontroli wersji, ale do ich skutecznego działania konieczne jest przeprowadzenie migracji wszystkich posiadanych plików.

### **Hybrydowe rozwiązania w chmurze/lokalne**

W celu usunięcia kilku oczywistych niedostatków usług typu cloud skierowanych do przedsiębiorstw kilku producentów wprowadziło na rynek hybrydowe rozwiązania mobilnego dostępu i udostępniania plików. Mimo, że tego rodzaju usługi dążą do przeniesienia większości plików użytkownika do chmury, to pozwalają także, aby organizacje przechowywały część swoich plików w usłudze typu cloud dostawcy, a resztę w należących do organizacji, lokalnych centrach danych.

Umożliwienie wykorzystania własnej infrastruktury centrów danych do celów mobilnego dostępu i udostępniania plików oznacza, że rozwiązania hybrydowe są krokiem we właściwym kierunku. Przechowywanie lokalne to w końcu nie tylko lepsza kontrola i nadzór nad plikami, ale także ułatwienie uzyskania zgodności z przepisami. Niestety, rozwiązania hybrydowe odziedziczyły też wiele wad cechujących usługi typu cloud skierowane do przedsiębiorstw.

### **Alokacja zasobów nowej i osobnej pamięci masowej**

Mimo że usługi hybrydowe pozwalają firmom na wykorzystanie własnych centrów danych i wyposażenia, firmy te muszą przydzielić nowe, odrębne zasoby pamięci masowej na potrzeby przechowywania danych mobilnych. Przenoszenie terabajtów danych ze starego do nowego magazynu w ramach wewnętrznej infrastruktury firmy jest oczywiście zadaniem mniej karkołomnym od przesyłania ich przez Internet. Nadal aktualne pozostają jednak kwestie wyboru plików do przeniesienia, wskazania podmiotu, który je przeniesie oraz określenia sposobu radzenia sobie z ich możliwą duplikacją.

### **Brak rzeczywistej integracji z obecnym systemem plików**

Większym problemem jest fakt, że nawet jeśli dane mobilne znajdują się w firmie, to mobilne udziały plikowe pozostają niezintegrowane z pozostałymi udziałami. Część rozwiązań hybrydowych umożliwia pewien stopień integracji z usługą Active Directory, ale nadal trzeba radzić sobie z nowym systemem plików. W takiej sytuacji firmy ponownie stają wobec konieczności wykonania znacznej pracy i odtworzenia oraz przekonfigurowania wszystkich posiadanych mechanizmów kontroli dostępu do plików dla danych przenoszonych do nowego systemu.

Teraz, zamiast zarządzać infrastrukturą z jednym systemem plików, trzeba zarządzać dwoma osobnymi infrastrukturami. Podobnie jak w przypadku usług w chmurze dla przedsiębiorstw, zarządzanie rozwiązaniem hybrydowym będzie oznaczać skorzystanie z osobnego zestawu narzędzi do zarządzania.

### **Inwestycja w dodatkowe procesy zarządzania danymi**

Usługi hybrydowe podnoszą stopień skomplikowania twojego środowiska. W rzeczywistości nie wykorzystują one usług plików istniejących w Twojej firmie, więc nie używają też żadnego z wdrożonych w niej procesów zarządzania danymi. Oto przykład — jak zrobić kopię zapasową danych z tych nowych mobilnych repozytoriów? Jak wiele pracy trzeba będzie włożyć w przebudowanie posiadanych usług tworzenia kopii zapasowych, aby mogły objąć także nowe magazyny danych? Czy konieczna będzie inwestycja w opracowanie nowych usług tworzenia kopii zapasowych? Które z pozostałych przepływów pracy oraz usług będą wymagać modyfikacji, aby mogły objąć swym działaniem hybrydowe rozwiązanie mobilnego dostępu do plików i udostępniania?

### **Rozwiązania lokalne zintegrowane z systemem plików**

Opisane dotąd rozwiązania i usługi mające przynieść większą wydajność pracowników mobilnych wystawiają organizację na wyższe ryzyko, komplikują zarządzanie, nie spełniają potrzeb użytkowników lub łączą w sobie wszystkie te problemy. Najlepszym sposobem na uniknięcie pułapek

związanych z mobilnym dostępem do plików i ich udostępnianiem jest sięgnięcie po rozwiązanie, które pozwala po prostu korzystać z plików i systemów plików posiadanych już przez organizację.

### Wykorzystanie posiadanych plików, systemów plików, procesów i funkcji kontroli

Bez względu na to, czy dotyczy to rozwiązań opartych na chmurze, czy wdrażanych lokalnie, użytkownikom chcącym korzystać z danych w ruchu niepotrzebny jest kolejny zestaw plików czy nowe repozytorium. Wystarczy, że będą mogli uzyskać dostęp do swoich plików w miejscu, w którym się one już znajdują i stamtąd udostępnić je innym. Działy IT nie chcą ani nie potrzebują kolejnego systemu plików, którym trzeba zarządzać, nie wspominając nawet o potrzebie zastosowania do tego celu całkowicie nowych narzędzi. Chcą tylko uzyskać mobilność posiadanych systemów plików, stosując do tego metody oparte na wykorzystaniu posiadanej infrastruktury zabezpieczeń, funkcji kontroli dostępu do plików oraz procesów zarządzania, w które już zainwestowano.

### Udostępnianie z funkcjami współpracy i nie tylko

Nawet w przypadku lokalnych rozwiązań zintegrowanych z systemem plików konieczne jest sprawdzenie, czy oferują one wszystkie wymagane przez użytkowników funkcje. Czy oprócz intuicyjnego, mobilnego dostępu do plików pozwalają na korzystanie z własnej infrastruktury bezpieczeństwa? Czy dokładność mechanizmów kontroli mobilnego udostępniania i pobierania jest wystarczająca, by spełnić wymagania zgodności ze standardami i zasadami firmy? Czy wybrane rozwiązanie pozwala użytkownikom mobilnym na szybkie i łatwe wyszukiwanie zawartości we wszystkich udziałach plikowych, do których mają prawo dostępu? Czy posiada ono wbudowane funkcje grupowego dzielenia się plikami, czy też zmusi użytkowników chcących uzupełnić udostępniane przez siebie pliki o określony kontekst, by sięgnęli do poczty e-mail i innych dróg komunikacji?

Jednym rozwiązaniem, które sprawdzi się we wszystkich wymienionych dziedzinach, jest Micro Focus® Filr. To wdrażane lokalnie rozwiązanie całkowicie integruje się z systemem plików i zapewnia użytkownikom potrzebne funkcje mobilnego korzystania z plików oraz ich udostępniania w ramach pracy grupowej.

### Mobilny dostęp do plików i udostępnianie pod kontrolą działu IT

Rozwiązanie Filr pozwala użytkownikom na łatwy dostęp mobilny do firmowych plików z dowolnego miejsca i za pomocą dowolnego urządzenia, a jednocześnie gwarantuje utrzymanie tego procesu pod kontrolą działu IT. Zapewnia ono wymagany przez użytkowników mobilny dostęp do plików i możliwość ich wymiany w grupie, używając jednak mechanizmów spełniających standardy korporacyjne i wykorzystując istniejącą infrastrukturę i funkcje kontroli. Pozwalając korzystać z posiadanych plików, serwerów plików oraz uprawnień do systemu plików, eliminuje konieczność zarządzania usługami innych dostawców, tworzenia hybrydowych magazynów i zarządzania nimi.

Zarówno w przypadku rozwiązań opartych na chmurze, jak i wdrażanych lokalnie, producenci systemów mobilnego dostępu do plików wiele

obiecują. Ich propozycje nie mogą jednak równać się z właściwie wyważonym podejściem rozwiązania Filr, które oferuje następujące korzyści:

- Wykorzystanie istniejących funkcji kontroli dostępu i przydziałów oraz zgodność z nimi, co pozwala, by zasady rządzące indywidualnym i grupowym dostępem do katalogów domowych i folderów sieciowych były stosowane także do dostępu mobilnego
- Płynną integrację z istniejącymi folderami użytkowników, w tym z katalogami domowymi i udziałami sieciowymi, dzięki której już od chwili uruchomienia rozwiązania zyskują oni bezpieczny dostęp mobilny do wszystkich swoich materiałów służbowych
- Uwierzytelniony dostęp i tworzenie śladu audytu z wykorzystaniem istniejących poświadczeń dostępu do plików
- Zarządzanie połączeniami między istniejącymi serwerami plików i punktami końcowymi, w tym komputerami z systemem Windows, Mac, iOS, Android, BlackBerry i Windows Mobile, a także standardowymi przeglądarkami internetowymi
- Nieinwazyjną i łatwą do zainstalowania maszynę wirtualną, która nie wymaga wdrażania agentów na serwerach, rozbudowy schemy ani inwestycji w nowy sprzęt do centrum danych
- Obsługa wielu magazynów tożsamości, w tym Microsoft Active Directory i Micro Focus eDirectory™
- Integrację z macierzystymi systemami plików w systemach Microsoft Windows Server i Micro Focus Open Enterprise Server (CIFS oraz NCP)
- Brak konieczności migrowania lub powielania plików, ponieważ pozostają one na istniejących firmowych serwerach plików
- Łatwe w użyciu funkcje synchronizacji plików z wszystkimi urządzeniami użytkownika
- Szczegółową kontrolę nad mobilnym pobieraniem plików
- Szczegółową kontrolę nad udostępnianiem plików, w tym możliwość decydowania, które z plików i folderów mogą być wewnętrznie i zewnętrznie udostępniane przez użytkowników

### Kontrola w rękach działu IT, zadowolenie użytkowników

Wyjątkowość rozwiązania Filr na tle innych rozwiązań mobilnego dostępu i grupowego udostępniania plików polega na tym, że zostało ono zaprojektowane z myślą o biznesie i o użytkownikach. W praktyce oznacza to mniejsze obciążenia dla administratorów, wyższy poziom bezpieczeństwa i większe zadowolenie pracowników. Filr pozwala wykorzystać istniejące w firmie mechanizmy zabezpieczeń i ochrony danych, dając jednocześnie użytkownikom potrzebną im łatwość dostępu do plików z dowolnego miejsca i przy użyciu dowolnego urządzenia. W rezultacie żądania użytkowników są zaspokojone, a ty zachowujesz kontrolę nad zapisaną w postaci plików własnością intelektualną firmy.

Aby dokładniej zapoznać się z tematem podnoszenia produktywności użytkowników i oszczędzania ich czasu dzięki dostarczeniu im rozwiązania mobilnego dostępu do plików i grupowego udostępniania, które nie narusza celów przedsiębiorstwa, odwiedź stronę [www.novell.com/filr](http://www.novell.com/filr) lub skontaktuj się z nami pod bezpłatnym numerem infolinii 800 226685.



**Micro Focus  
Polska**

+48 22 537 5000

**Micro Focus  
Kwatera główna**

Wielka Brytania  
+44 (0) 1635 565200

**[www.novell.com](http://www.novell.com)**