Microsoft

Zarządzanie dostępem do aplikacji i zabezpieczanie go za pomocą usługi Azure Active Directory

Sekcja 1

Co to jest zarządzanie dostępem i tożsamościami?

Co to jest zarządzanie dostępem i tożsamościami?

Cyfrowa transformacja

Przetwarzanie w chmurze i urządzenia przenośne przeobraziły nowoczesne miejsce pracy. Coraz bardziej globalni pracownicy mogą elastycznie pracować w dowolnym miejscu przy użyciu bezpłatnych i niedrogich aplikacji SaaS („oprogramowanie udostępniane jako usługa”), które pozwalają sprostać wyzwaniom związanym z wydajnością i współpracą. Duże przedsiębiorstwa migrują aplikacje i procesy obliczeniowe do chmury, aby modernizować swoją architekturę, a różne specjalizacje biznesowe korzystają z nowych usług w chmurze do tworzenia niestandardowych aplikacji dostosowanych do ich konkretnych potrzeb. Przedsiębiorstwa skorzystały na nadejściu nowych technologii przez zwiększenie wydajności, ale cyfrowa transformacja postawiła przed nimi także trzy nowe wyzwania.

Co to jest zarządzanie dostępem i tożsamościami?

Nowe wyzwania

Czynnik ryzyka: przed rewolucją związaną z chmurą rozwiązania informatyczne pełniły funkcję strażników technologii. Aplikacje i platformy zarządzane i zabezpieczane przez organizację znajdowały się wewnątrz sieci obwodowej, a każda osoba logująca się do zasobów firmy była najpierw weryfikowana przez zaporę. Te dni minęły. Pracownicy mają teraz szerszą kontrolę nad używaną przez nich technologią, która w znacznym stopniu jest dostępna za pośrednictwem Internetu. Cyberprzestępcy nauczyli się wykorzystywać te luki w zabezpieczeniach. Nawet jeśli użytkownik zna poprawne hasło do konta, nie zawsze można mieć pewność, że jest on tym, za kogo się podaje.

Problem administracyjny: gwałtowny wzrost liczby punktów końcowych zapewnia użytkownikom więcej sposobów łączenia się i komunikowania, ale skutkuje też prawdziwym koszmarem administracyjnym. Wiele przedsiębiorstw nie wie o wszystkich narzędziach, z których korzystają pracownicy, a nawet jeśli mają one solidny spis tych narzędzi, już sama liczba aplikacji w chmurze sprawia, że trzeba zarządzać wieloma systemami tożsamości, co zwiększa koszty i dokłada się jeszcze do już istniejących zagrożeń dla bezpieczeństwa.

Fatalne środowisko użytkownika: użytkownicy też są niezadowoleni. Uwielbiają elastyczność, ale są sfrustrowani liczbą poświadczeń, które muszą pamiętać.

Czynnik ryzyka

Problem administracyjny

Fatalne środowisko użytkownika

Co to jest zarządzanie dostępem i tożsamościami?

Zarządzanie tożsamością i dostępem jako centralna płaszczyzna kontroli

Wspólnym mianownikiem wszystkich tych problematycznych kwestii są nieefektywne systemy weryfikacji tożsamości. Tożsamość zastąpiła sieć obwodową jako nowa płaszczyzna kontroli. Potrzebne są rozwiązania łączące różne narzędzia, architekturę, urządzenia i usługi w całym przedsiębiorstwie, aby umożliwić lepszą ochronę organizacji i zarządzanie dostępem zarówno pracowników, jak i partnerów zewnętrznych — systemy zarządzania tożsamością i dostępem (IAM, Identity and Access Management) łączą funkcje dostępu w ramach jednego systemu, zapewniając większą kontrolę. Umożliwiają one bezproblemową współpracę ponad granicami organizacji, jednocześnie wzmacniając zabezpieczenia zasobów korporacyjnych. Dobre rozwiązanie IAM pozwala połączyć użytkowników ze wszystkimi aplikacjami służbowymi — bez względu na to, czy są one hostowane w chmurze, czy w środowisku lokalnym — za pomocą jednego zestawu poświadczeń. Zadaniem rozwiązań IAM jest zapewnianie użytkownikom dostępu tylko do potrzebnych im zasobów i blokowanie nieautoryzowanym użytkownikom dostępu do danych, do których nie powinni go mieć. Prawami dostępu i uprawnieniami użytkowników zarządza się w scentralizowanym portalu przy ograniczeniu wielu ręcznych procesów związanych z aprowizowaniem i cofaniem aprowizacji kont użytkowników. Rozwiązania IAM zapewniają również narzędzia do zarządzania zasadami zabezpieczeń dotyczącymi tożsamości i aplikacji. Najlepsze rozwiązania IAM lepiej chronią tożsamości, usprawniają środowisko użytkownika i zwiększają wydajność administrowania.

Rozwiązania IAM pozwalają sprostać tym wyzwaniom

Lepsza ochrona tożsamości

Usprawnione środowisko użytkownika

Wydajniejsze administrowanie

Sekcja 2

Omówienie usługi Azure AD

Omówienie usługi Azure AD

Kompleksowe rozwiązanie

Usługa Microsoft Azure Active Directory (Azure AD) to kompleksowe rozwiązanie IAM w chmurze oraz lider na rynku rozwiązań do obsługi zarządzania katalogami, dostępu do aplikacji i zaawansowanej ochrony tożsamości. Usługa Azure AD zwiększa możliwości organizacji w zakresie zarządzania tożsamościami pracowników, partnerów i klientów oraz ich zabezpieczania na potrzeby dostępu do aplikacji i usług. Usługa Azure AD pomaga milionom organizacji zarządzać ponad miliardem tożsamości i zabezpieczać je.

Modernizacja dostępu

Zarządzaj dostępem do danych i zasobów organizacji — lokalnych i w chmurze — i zabezpieczaj je. Połącz wszystkich użytkowników oraz wszystkie aplikacje i urządzenia z chmurą, aby zapewniać sprawny, bezpieczny dostęp oraz lepszy wgląd w informacje i kontrolę. Automatyzacja przepływów pracy i udostępnienie opcji samoobsługi pozwala obniżać koszty i zwiększać wydajność użytkowników.

Zabezpieczanie i administrowanie

Przy bardzo dużej liczbie ataków na poświadczenia użytkowników występujących każdego dnia właściwym sposobem zapobiegania naruszeniom jest ciągłe śledzenie normalnego i nienormalnego zachowania w zakresie najszerszego możliwego zestawu sygnałów, stosowanie sztucznej inteligencji i automatyzacja reakcji. Ważne jest zachowanie równowagi między produktywnością a zabezpieczeniami dzięki sprawnemu dostępowi do odpowiednich zasobów oraz regularnym przeglądom dostępu i egzekwowaniu zasad.

Współtworzenie i współpraca

Rozwijaj swoją firmę dzięki niezawodnej usłudze w chmurze, którą można skalować do milionów użytkowników i która zapewnia wiodące w branży zabezpieczenia i elastyczność. Zapewnij łączność użytkownikom zewnętrznym i ułatw im zwiększenie produktywności dzięki przyjaznym, samoobsługowym środowiskom i wbudowanym mechanizmom zabezpieczeń.

Tworzenie rozwiązań i integracja

Twórz aplikacje, do których użytkownicy łatwo zalogują się za pomocą kont osobistych Microsoft, kont służbowych lub kont społecznościowych. Połącz się z usługą Microsoft Graph, bramą do danych i analiz na platformie Microsoft 365, i twórz rozbudowane aplikacje. Dodaj obsługę logowania jednokrotnego i zautomatyzuj aprowizowanie użytkowników — działaj tak jak największe organizacje na świecie.

Sekcja 3

Usługa Azure AD dla Twoich aplikacji

Usługa Azure AD dla Twoich aplikacji

Uniwersalna platforma

Usługa Azure AD pozwala zarządzać wspólną tożsamością dla każdego użytkownika w całej infrastrukturze hybrydowej organizacji, umożliwiając mu uzyskiwanie dostępu do wszystkich potrzebnych mu aplikacji, w tym do aplikacji biznesowych hostowanych lokalnie i w chmurze. Zarządzaj wszystkimi tożsamościami organizacji na uniwersalnej platformie, która zwiększa wydajność administracyjną i zapewnia Ci większą kontrolę. Stosuj szczegółowe zasady zabezpieczeń do każdej aplikacji używanej w organizacji.

Usługa Azure AD dla Twoich aplikacji

Oszczędność czasu i pieniędzy

Usługa Azure AD jest wstępnie zintegrowana z tysiącami aplikacji, w tym tymi bardzo popularnymi, takimi jak Workday, ServiceNow, SuccessFactors, Adobe i Concur, dzięki czemu łatwiej udostępnisz te aplikacje użytkownikom. Za pomocą jednej konsoli wdrożysz spójne zasady i będziesz skutecznie monitorować prawa dostępu. Możesz zautomatyzować przepływy pracy dotyczące aprowizowania użytkowników i zarządzania cyklem eksploatacji, a także zaoszczędzić czas i zasoby dzięki samoobsługowemu zarządzaniu kontami. Możesz również pobierać informacje o użytkownikach z narzędzi działu kadr i traktować je jako źródło prawdziwych danych, eliminując potrzebę stosowania skryptów niestandardowych i ręcznych procesów do zarządzania atrybutami użytkownika.

Aplikacje konfigurowane za pomocą usługi Azure AD mogą obsługiwać logowanie jednokrotne zapewniające sprawny dostęp. Oznacza to, że użytkownicy nie muszą pamiętać poświadczeń dla każdego konta aplikacji ani ponownie wykorzystywać słabych haseł i ryzykować wystąpienie naruszenia danych. Konta, dla których skonfigurowano automatyczne aprowizowanie, zapewniają użytkownikom dostęp do nowych zasobów tak szybko, jak to tylko możliwe. W przypadku obsługi aprowizacji przychodzącej usługa Azure AD zapewnia nowym pracownikom dostęp do wszystkich odpowiednich zasobów już pierwszego dnia.

Oszczędność czasu i pieniędzy

Wbudowane integracje SaaS

Logowanie jednokrotne

Dostęp dla użytkowników od pierwszego dnia

Usługa Azure AD dla Twoich aplikacji

Zapewnianie bezpieczniejszego dostępu do wszystkich aplikacji

Usługa Azure AD zapewnia kompleksową ochronę tożsamości we wszystkich aplikacjach — zarówno w aplikacjach SaaS, jak i w lokalnych aplikacjach biznesowych. Niezależnie od tego, czy użytkownik żąda dostępu do programu Microsoft Word, czy do usługi Box, usługa Azure AD zapewnia potwierdzenie tożsamości przed udzieleniem dostępu. Można także ustanowić zasady administrowania dostępem, aby zapewnić użytkownikom dostęp tylko do tego, czego potrzebują, gdy tego potrzebują. Można wymagać od użytkowników, aby zwracali się o uprawnienia dostępu, ustalić limit czasu, przez jaki będą mogli uzyskiwać dostęp do aplikacji, oraz przeprowadzać regularne przeglądy zgodności w zakresie dostępu.

Ponadto usługa Azure AD wykorzystuje możliwości usługi Microsoft Intelligent Security Graph i uczenia maszynowego do analizowania bilionów sygnałów we wszystkich naszych produktach i usługach w celu wykrywania nietypowych zachowań i przypisywania względnego ryzyka każdej sesji. Aby ocenić ryzyko logowania, usługa Azure AD uwzględnia urządzenie, lokalizację i inne informacje kontekstowe. Można ustanowić zasady dostępu warunkowego usługi Azure AD, które automatycznie stosują mechanizmy zabezpieczeń, takie jak blokowanie żądania dostępu lub wymaganie zresetowania hasła, gdy logowanie zostało uznane za ryzykowne lub spełnione są określone warunki zasad.

Mechanizmy zabezpieczania aplikacji

Ochrona tożsamości

Administrowanie dostępem

Zasady dostępu warunkowego

Sekcja 4

Jak zarządzać aplikacjami i zabezpieczać je za pomocą usługi Azure AD

Usługa Azure AD ułatwia zachowanie kontroli i zmniejszenie kosztów dzięki automatyzacji, samoobsłudze i egzekwowaniu zasad.

Jak zarządzać aplikacjami i zabezpieczać je za pomocą usługi Azure AD

Integracje aplikacji z usługą Azure AD

Galeria aplikacji usługi Azure AD ułatwia skonfigurowanie i połączenie dowolnej z tysięcy wstępnie zintegrowanych aplikacji z dzierżawą organizacji. Wszystkie te aplikacje obsługują logowanie jednokrotne i można łatwo skonfigurować w nich dostęp warunkowy usługi Azure AD — dla poszczególnych aplikacji lub za pomocą zasad obowiązujących w całym przedsiębiorstwie. Po dodaniu aplikacji i skonfigurowaniu jej stosownie do potrzeb użytkownicy z autoryzowanym dostępem łatwo znajdą ją w portalu Moje aplikacje usługi Azure AD — scentralizowanym portalu do wyszukiwania i uruchamiania aplikacji dla użytkowników końcowych.

Jeśli masz opracowaną aplikację lub potrzebujesz aplikacji zintegrowanej ze swoją organizacją, możesz również poprosić o dodanie jej do galerii aplikacji usługi Azure AD.

Przeglądaj tysiące wstępnie zintegrowanych aplikacji >

Bezpieczny dostęp hybrydowy

Serwer proxy aplikacji usługi Azure AD pozwala zapewniać bezpieczny dostęp zdalny do lokalnej aplikacji internetowej opartej na oświadczeniach bez potrzeby stosowania sieci VPN. Serwer proxy aplikacji wymaga zainstalowania lekkiego łącznika i zapewnia to samo środowisko informatyczne i użytkownika końcowego co aplikacje SaaS łączące się za pośrednictwem galerii aplikacji usługi Azure AD.

Natomiast jeśli chcesz wykorzystać istniejące inwestycje w infrastrukturę, na przykład uzyskane od partnerów takich jak F5 ZScaler, SAP, Oracle i Ping Identity, aby połączyć innego typu aplikacje, na przykład używające protokołów uwierzytelniania opartych na nagłówkach lub protokołu Kerberos, możesz to zrobić i nadal zyskać korzyści związane z centralizacją i zabezpieczeniami usługi Azure AD.

Przeczytaj, jak dodać aplikację lokalną za pośrednictwem serwera proxy aplikacji >

Łączenie innych partnerskich chmur i sieci aplikacji >

Jak zarządzać aplikacjami i zabezpieczać je za pomocą usługi Azure AD

Zautomatyzowane aprowizowanie

Usługa Azure AD pozwala zautomatyzować tworzenie, konserwowanie i usuwanie tożsamości użytkowników w popularnych aplikacjach SaaS. Możesz automatycznie tworzyć nowe konta w odpowiednich systemach dla nowych osób dołączających do Twojego zespołu lub organizacji. Możesz też skonfigurować zasady automatycznie dezaktywujące konta osób opuszczających Twój zespół lub organizację z odpowiednich systemów. Automatyzacja tych zadań zapewnia, że tożsamości w aplikacjach i systemach będą aktualizowane na podstawie zmian w katalogu lub używanym systemie zarządzania kadrami, co pozwala zmniejszyć liczbę błędów i oszczędzić czas.

Dowiedz się więcej o konfigurowaniu zautomatyzowanego udostępniania i cofania aprowizacji aplikacji SaaS >

Zarządzanie grupami

Usługa Azure AD ułatwia zapewnianie dostępu do zasobów organizacji, udzielając praw dostępu pojedynczemu użytkownikowi lub całej grupie usługi Azure AD. Korzystanie z grup umożliwia właścicielowi zasobu ustawianie uprawnień dostępu dla wszystkich członków grupy naraz zamiast pojedynczo. Jest to bezpieczniejsza metoda, ponieważ zmniejsza prawdopodobieństwo przypadkowego udzielenia niewłaściwego dostępu jakiejś osobie. Pozwala też zaoszczędzić czas. Można także dynamicznie skalować zarządzanie grupami, automatyzując rejestrację za pomocą zasad opartych na atrybutach tożsamości.

Dowiedz się, jak utworzyć grupę w witrynie Azure Portal >

Jak zarządzać aplikacjami i zabezpieczać je za pomocą usługi Azure AD

Samoobsługa użytkowników

Niektórych zadań nie muszą wykonywać informatycy, a usługa Azure AD umożliwia delegowanie tego typu zadań do innych osób w organizacji. Użytkowników można upoważnić do tworzenia własnych grup zabezpieczeń i do zarządzania nimi w usłudze Azure AD. Właściciele grup mogą zatwierdzać lub odrzucać wnioski o członkostwo. Mogą też delegować kontrolę nad członkostwem w grupie.

Konfigurowanie grup zarządzanych samodzielnie >

Samoobsługa obejmuje również użytkowników. Użytkownicy mogą tworzyć konta za pośrednictwem portalu samoobsługowego, jeśli mają zweryfikowane adresy e-mail. Za pomocą tego portalu mogą też resetować hasła. Może to zaoszczędzić działowi pomocy technicznej mnóstwo czasu i pieniędzy.

Konfigurowanie samoobsługowego resetowania haseł >

Modernizacja uwierzytelniania

Jeśli obecnie używasz uwierzytelniania lokalnego, takiego jak usługi federacyjne w usłudze Active Directory (AD FS, Active Directory Federation Services), rozważ migrację aplikacji do usługi Azure AD. Pozwoli Ci to zachować korzyści dotyczące użytkowników, takie jak logowanie jednokrotne, a jednocześnie zyskasz skalowalność i związane z zabezpieczeniami korzyści dostępne w chmurze, takie jak stosowanie szczegółowych mechanizmów kontroli dostępu dla poszczególnych aplikacji za pomocą dostępu warunkowego usługi Azure AD lub udzielanie partnerom dostępu do zasobów za pomocą funkcji współpracy B2B usługi Azure AD. Migrować można wszystkie aplikacje korzystające ze standardów SAML 2.0, WS-Federation, OAuth i OpenID Connect do logowania federacyjnego.

Tworzenie zasad dostępu warunkowego usługi Azure AD w celu zabezpieczania dostępu do aplikacji >

Bezproblemowa współpraca z partnerami zewnętrznymi dzięki funkcjom B2B usługi Azure AD >

Bezpiecznie połącz dowolną aplikację w dowolnej chmurze lub na dowolnym serwerze z usługą Azure AD.

1 milion aktywnych unikatowych połączonych aplikacji.

Microsoft

Zacznij korzystać już dziś.

Rozpocznij bezpłatny miesięczny okres próbny usługi Azure AD, aby przekonać się, jak łatwo jest zarządzać dostępem użytkowników do wszystkich aplikacji i zabezpieczać przedsiębiorstwo.