



Azure Active Directory ile uygulamalarınıza erişimi yönetin ve güvenli hale getirin



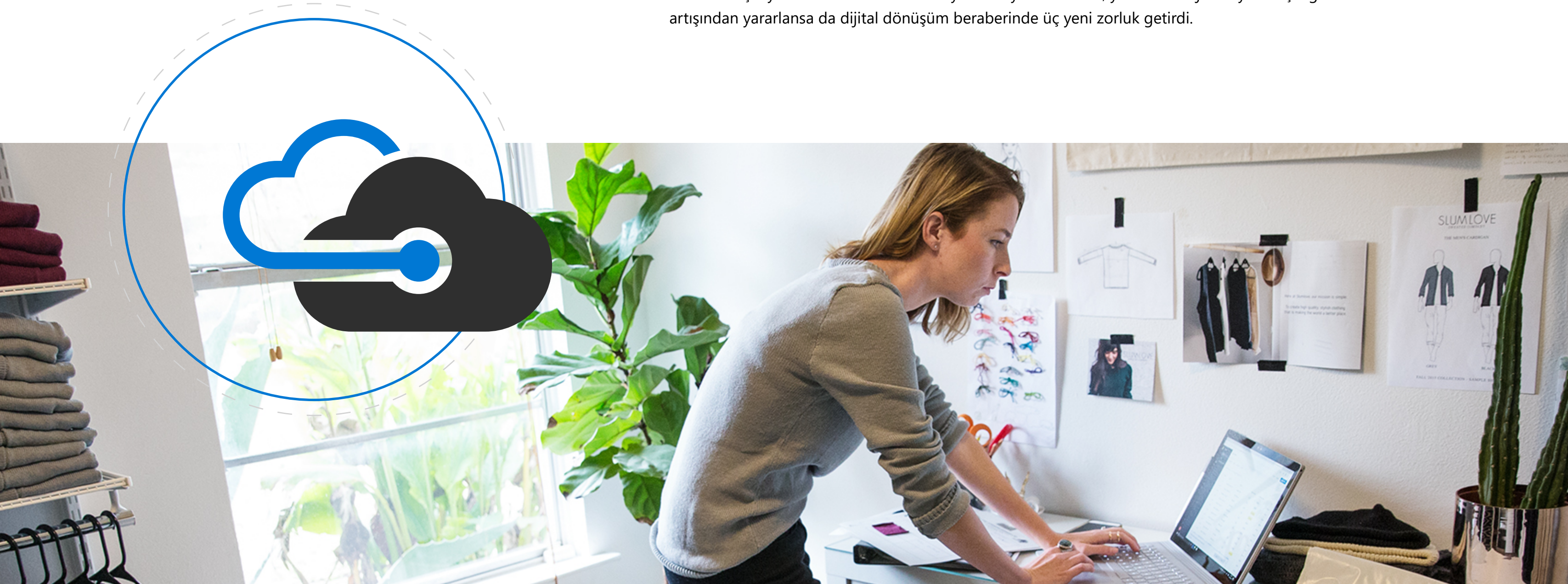
Bölüm 1

Kimlik ve erişim
yönetimi nedir?

Kimlik ve erişim yönetimi nedir?

Dijital dönüşüm

Bulut bilişim ve mobil cihazlar, modern işyerini dönüştürdü. Giderek küresel hale gelen işgücü, üretkenlik ve işbirliğiyle ilgili zorlukların üstesinden gelmek için ücretsiz ve düşük maliyetli hizmet olarak yazılım (SaaS) uygulamalarını kullanarak her yerden çalışma esnekliğine sahiptir. Büyük kurumlar mimarilerini modernleştirmek için uygulamalarını ve bilgi işlemlerini buluta geçiriyor ve iş kolları, belirli ihtiyaçlarına yönelik özel uygulamalar derlemek için yeni bulut hizmetlerinden yararlanıyor. Kurumlar, yeni teknolojiye yükselişe gelen üretkenlik artışından yararlansa da dijital dönüşüm beraberinde üç yeni zorluk getirdi.



Kimlik ve erişim yönetimi nedir?

Yeni zorluklar

Dijital dönüşüm
kaynaklı zorluklar

Güvenlik riski: Bulut devriminden önce BT'nin görevi teknoloji bekçiliği idi. Yönetip güvenliğini sağladığınız uygulama ve platformlar ağ çevresine dahildi ve kurumsal kaynaklarınızda oturum açan herkes ilk önce güvenlik duvarı tarafından doğrulanırdı. Artık bu günler geride kaldı. İşgücünüz kullandığı teknoloji üzerinde çok daha fazla denetime sahip ve bu teknolojinin büyük kısmına internet üzerinden erişiliyor. Siber saldırganlar, bu güvenlik açıklarından yararlanmayı öğrendi. Bir kullanıcı bir hesabın doğru parolasını bilse bile bu kullanıcının belirttiği kişi olduğundan her zaman emin olmak mümkün değildir.

Yönetim açısından zorluk: Uç nokta sağlayıcılarının sayısında yaşanan büyük artış kullanıcılara daha çok sayıda bağlantı yöntemi sağlasa da yönetsel açıdan bir kabus yaratır. Birçok kurum, çalışanların kullandığı tüm araçlar hakkında bilgi sahibi değildir. İyi bir envanterleri olduğunda bile bulut uygulamalarının sayısı, birden fazla kimlik sistemini yönetmeniz gerektiği anlamına gelir ve bu da hem maliyetleri hem de mevcut güvenlik risklerini artırır.

Olumsuz kullanıcı deneyimi: Kullanıcılar da zorluk çeker. Esnekliği sevseler de hatırlamaları gereken çok fazla kimlik bilgisi olmasını istemezler.



Güvenlik riski



Yönetim açısından
zorluk



Olumsuz kullanıcı
deneyimi

Kimlik ve erişim yönetimi nedir?

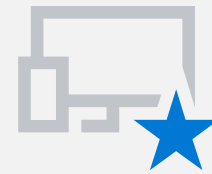
Merkezi denetim düzlemi olarak kimlik ve erişim yönetimi

Bu sorunların ortak noktası, kimlik doğrulama sistemlerinin verimsizliğidir. Kimlik, yeni kontrol düzlemi olarak ağ çevresinin yerini aldı. Kurumu daha iyi koruyup hem çalışanlar hem de dış iş ortakları için erişimi yönetmek amacıyla kurum genelinde farklı araçları, mimarileri, cihazları ve hizmetleri bağlayan çözümlere ihtiyacınız vardır. Kimlik ve erişim yönetimi (IAM) sistemleri de erişimi tek bir sistem altında birleştirerek size daha fazla denetim sunar. Bu çözümler, kurumsal kaynaklarınızın güvenliğini artırırken kurumunuz dahilindeki her noktada sorunsuz işbirliği sağlar. İyi bir IAM çözümü, tek bir kimlik bilgileri kümesi aracılığıyla, bulutta ya da şirket içinde olmaları fark etmeksizin kullanıcılarınızı tüm iş uygulamalarına bağlamanıza imkan tanır. IAM çözümleri, kullanıcılara yalnızca ihtiyaç duydukları kaynaklara erişim vermek ve yetkisiz kullanıcıların erişmemeleri gereken verilere erişmesini engellemek üzere tasarlanmıştır. Merkezi bir portaldan kullanıcı erişim haklarını ve izinlerini yönettiğinizden kullanıcı hesaplarının sağlanması ve sağlamanın kaldırılmasıyla ilgili el ile gerçekleştirilen süreçlerin birçoğu ortadan kalkar. IAM çözümleri aynı zamanda kimlikleriniz ve uygulamalarınız genelinde güvenlik ilkelerini yönetmenize imkan tanıyan araçlar da sağlar. En iyi IAM çözümleri, kimlikleri daha iyi korur, kullanıcı deneyimini geliştirir ve yönetim verimliliğini artırır.

IAM çözümleri bu
zorlukları ortadan
kaldırır



Kimlikleri daha
iyi koruyun



Kullanıcı deneyimini
geliştirin



Yönetim verimliliğini
artırın

Bölüm 2

Azure AD'ye Genel Bakış

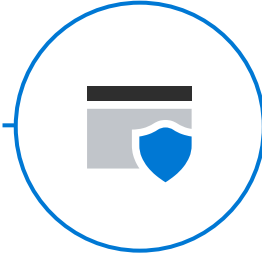
Kapsamlı bir çözüm

Bulutta kapsamlı bir IAM çözümü olan Microsoft Azure Active Directory (Azure AD) dizinleri yönetme, uygulama erişimi ve gelişmiş kimlik koruması açısından pazar lideridir. Azure AD sayesinde kurumlar çalışanları, iş ortakları ve müşterileri için kimlikleri yönetip bunların güvenliğini sağlayabilir, ihtiyaç duydukları uygulama ve hizmetlere erişebilir. Azure AD, milyonlarca kurumun bir milyardan fazla kimliği yönetip bunların güvenliğini sağlamasına yardımcı olur.



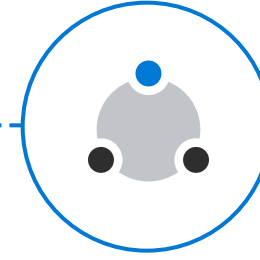
Erişimi modernleştirin

Kurumunuzun hem şirket içindeki hem de buluttaki verilerine ve kaynaklarına erişimi yönetip bunun güvenliğini sağlayın. Sorunsuz ve güvenli erişimin yanı sıra daha fazla görünürlük ve denetim için tüm kullanıcılarınızı, uygulamalarınızı ve cihazlarınızı buluta bağlayın. İş akışlarını otomatikleştirin ve self servis seçeneklerin maliyetleri düşük düzeyde tutup kullanıcılarınız için üretkenliği artırmasına imkan tanıyın.



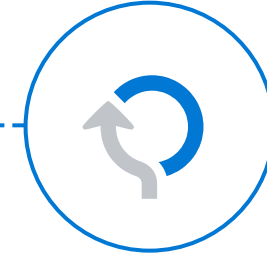
Koruyun ve yönetin

Her gün kullanıcı kimlik bilgilerini hedef alan saldırıların yüksek hacmi düşünüldüğünde gizlilik ihlali önlemenin yolu, mümkün olan en geniş sinyal kümesi genelinde normal ve anormal davranışları devamlı izlemek, yapay zekayı uygulamak ve yanıtları otomatikleştirmektir. Doğru kaynaklara zamanında erişim, düzenli erişim incelemeleri ve ilke uygulama sayesinde üretkenlik ve güvenlik arasında dengeyi yakalayın.



Bağlantı kurun ve işbirliği yapın

Sektör lideri güvenlik ve esneklik ile milyonlarca kullanıcıya ölçeklendirilebilen güvenilir bir bulut hizmeti ile işinizi büyütün. Dış kullanıcılarınızla bağlantı kurun ve kullanıcı dostu, self servis deneyimler ve yerleşik güvenlik denetimleri ile üretken olmaları için kullanıcılarınızı destekleyin.



Geliştirin ve bütünleştirin

Kullanıcılara Microsoft kişisel, iş veya okul hesaplarında ya da sosyal medya hesaplarında oturum açmalarının kolay bir yolunu sunan uygulamalar derleyin. Microsoft 365'teki veri ve zeka ağ geçidi olan Microsoft Graph'e bağlanmaya başlayın ve zengin uygulamalar derleyin. Çoklu oturum açmayı etkinleştirip kullanıcı sağlamayı otomatikleştirin ve dünyanın en büyük kurumlarına ulaşın.

Bölüm 3

Uygulamalarınız
için Azure AD

Uygulamalarınız için Azure AD

Evrensel platform

Azure AD, bulut ve şirket içi iş kolu uygulamaları dahil olmak üzere ihtiyaç duydukları tüm uygulamalara erişmeleri amacıyla hibrit altyapınız genelindeki her bir kullanıcı için bir genel kimliği yönetmenize imkan tanır. Tüm kimliklerinizi evrensel bir platformdan yöneterek yönetici verimliliğini artırın ve daha fazla denetim elde edin. Kurumunuzda kullanılan uygulamaların her birine ayrıntılı güvenlik ilkeleri ekleyin.



Uygulamalarınız için Azure AD

Zamandan ve paradan tasarruf edin

Azure AD; Workday, ServiceNow, SuccessFactors, Adobe ve Concur gibi popüler seçenekler dahil olmak üzere binlerce uygulama ile önceden bütünleştirildiğinden, bu uygulamaları kullanıcılarınıza daha kolay bir şekilde sunabilirsiniz. Tek bir konsol ile tutarlı ilkeler dağıtın ve erişim haklarını izleyin. Kullanıcı sağlama ve yaşam döngüsü yönetimi için iş akışlarını otomatikleştirebilir ve self servis hesap yönetimi ile zamandan ve kaynaktan tasarruf edebilirsiniz. Ayrıca gerçek bilgi kaynağı olarak İK araçlarından kullanıcı bilgilerini alıp kullanıcı özneliklerini yönetmek için özel betik veya el ile yürütülen süreç ihtiyacını ortadan kaldırabilirsiniz.

Azure AD ile yapılandırılan uygulamalar sorunsuz erişim için çoklu oturum açmayı (SSO) etkinleştirir. Yani kullanıcılar her bir uygulama için kimlik bilgilerini hatırlamak zorunda kalmaz veya zayıf parolaları tekrar kullanıp veri ihlali riski almaz. Otomatik sağlama için yapılandırılan hesaplar, kullanıcıların yeni kaynaklara mümkün olan en yakın zamanda erişmesini sağlar. Azure AD, gelen sağlama için yeni işe girenlerin ilk günden ilgili tüm kaynaklara erişmesini sağlar.



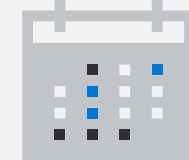
Zamandan ve
paradan tasarruf



Yerleşik SaaS
bütünleştirmeleri



Çoklu oturum
açma



İlk günden
kullanıcı erişimi

Uygulamalarınız için Azure AD

Tüm uygulamalarınız için daha güvenli erişim sağlayın

Azure AD, hem SaaS uygulamaları hem de şirket içi iş kolu uygulamalarınız dahil olmak üzere tüm uygulamalarınız için kapsamlı kimlik koruması sağlar. Kullanıcının Microsoft Word veya Box'a erişim isteğinde bulunması fark etmeksizin Azure AD, erişim vermeden kullanıcı kimliğinin doğrulanmasını sağlar. Ayrıca kullanıcıların yalnızca ihtiyaç duydukları şeylere gerektiği zamanda erişebilmesini sağlamak için erişim yönetimi ilkeleri de oluşturabilirsiniz. Kullanıcıların erişim izni istemesi şartını getirebilir ve ayrıca uygulama erişim sürelerini kısıtlayıp erişimleri düzenli olarak uyumluluk açısından inceleyebilirsiniz.

Azure AD, tipik olmayan davranışları tespit edip ilgili riski her bir oturuma atamak üzere tüm ürünlerimiz ve hizmetlerimiz genelinde trilyonlarca sinyali analiz etmek için Microsoft Intelligent Security Graph ve makine öğreniminin gücünden de yararlanır. Azure AD cihaz, konum ve diğer bağlamsal bilgilere bakarak oturum açmanın riskini değerlendirir. Bir erişim isteğini engelleme ya da bir oturum açma işlemi riskli görüldüğünde ya da belirli ilke koşulları karşılandığında parola sıfırlaması gerektirme gibi otomatik olarak güvenlik önlemleri için uygulanan Azure AD Koşullu Erişim ilkeleri oluşturabilirsiniz.



Uygulama
güvenlik önlemleri



Kimlik
koruması



Erişim yönetimi



Koşullu Erişim
ilkeleri

Bölüm 4

**Azure AD ile uygulamalar nasıl yönetilir
ve bunların güvenliği nasıl sağlanır?**

Azure AD, otomasyon, self servis ve ilke uygulamasından yararlanarak denetimi elde tutmayı ve maliyetleri azaltmayı kolaylaştırır.

Azure AD ile uygulamalar nasıl yönetilir ve bunların güvenliđi nasıl sađlanır?



Azure AD uygulama bütnleřtirmeleri

Azure AD uygulama galerisi, kiracınıza nceden btnleřtirilen binlerce uygulamadan herhangi birini yapılandırmayı ve buna bađlanmayı kolaylařtırır. Tm bu uygulamalar SSO deneyimini destekler. Ayrıca uygulama bařına řeklinde veya kurum genelindeki ilkeler iin Azure AD Kořullu Eriřim'e ynelik uygulamaları kolayca yapılandırabilirsiniz. Uygulamayı ekleyip ihtiyalarınıza gre yapılandırđınızda, yetkili eriřime sahip kullanıcılar, bu uygulamayı son kullanıcıların uygulamaları keřfedip bařlatmasına ynelik bir merkezi portal olan Azure AD My Apps portalında kolayca bulabilir.

Bir uygulama derlediyseniz ya da kurumunuz iin bir uygulamanın btnleřtirilmesine ihtiyacınız varsa bunun Azure AD uygulama galerisinde listelenmesini de isteyebilirsiniz.

[nceden btnleřtirilmiř binlerce uygulamayı keřfedin >](#)



Gvenli hibrit eriřim

Azure AD Uygulama Ara Sunucusu'nu kullanarak, VPN ihtiyacı olmadan řirket iindeki talep tabanlı web uygulamalarına gvenli ve uzaktan eriřim sađlayın. Uygulama Ara Sunucusu, basit bir bađlayıcı yklemesi gerektirir ve Azure AD uygulama galerisi aracılıđıyla bađlanan SaaS uygulamaları ile aynı BT ve son kullanıcı deneyimi sađlar.

st bilgi tabanlı veya Kerberos kimlik dođrulaması protokollerinden yararlanan uygulamalar gibi diđer uygulama trlerini bađlamak amacıyla F5 ZScaler, SAP, Oracle veya Ping Identity gibi iř ortaklarıyla mevcut altyapı yatırımlarından yararlanmak istiyorsanız bunu da yapabilir ve ayrıca Azure AD'nin merkezileřtirme ve gvenlik avantajlarından yararlanabilirsiniz.

[Uygulama Ara Sunucusu aracılıđıyla řirket ii uygulama ekleme hakkında bilgi edinin >](#)

[Diđer iř ortađı uygulama ađlarını ve bulutlarını bađlayın >](#)

Azure AD ile uygulamalar nasıl yönetilir ve bunların güvenliđi nasıl sađlanır?



Otomatikleřtirilmiř sađlama

Azure AD, popöler SaaS uygulamalarında kullanıcı kimliđi oluřturma, bakım ve kaldırma işlemlerini otomatikleřtirmenize imkan tanır. Ekibinize veya kurumunuza katılan yeni kişiler için otomatik olarak dođru sistemlerde yeni hesaplar oluřturabilirsiniz. Kiřiler ekibinizden veya kurumunuzdan ayrıldıđında hesaplarını dođru sistemlerde otomatik olarak devre dıřı bırakacak ilkeler belirleyebilirsiniz. Bu görevleri otomatikleřtirerek uygulamalarınız ve sistemlerinizdeki kimliklerinizin, dizindeki veya insan kaynakları sisteminizdeki deđiřikliklere göre güncel tutulmasını sađlayabilir, böylece hataları ve harcanan zamanı azaltabilirsiniz.

[SaaS uygulamalarına otomatik sađlama ve otomatik sađlamayı kaldırma ayarlama hakkında daha fazla bilgi edinin >](#)



Grup yönetimi

Azure AD, tek bir kullanıcıya ya da bir Azure AD grubunun tamamına erişim hakları vererek kurumunuzun kaynaklarına erişim vermenize yardımcı olur. Kaynak sahibinin grupları kullanması, hakları tek tek vermek zorunda kalmak yerine bir grubun tüm üyeleri için erişim izinleri ayarlamasına imkan tanır. Bu, bir bireye uygun olmayan erişim verme ihtimaliniz daha az olduđundan daha güvenli bir yöntemdir ve ayrıca size zaman kazandırabilir. Kimlik özniteliđi tabanlı ilkeler aracılıđıyla kayıt işleminin otomatik hale gelmesini sađlayarak grup yönetiminizi dinamik olarak ölçeklendirebilirsiniz.

[Azure portalında grup oluřturmayı öğrenin >](#)

Azure AD ile uygulamalar nasıl yönetilir ve bunların güvenliđi nasıl sađlanır?



Kullanıcı self servis

Bazı görevleri bir BT uzmanının tamamlaması gerekmez ve Azure AD bunları kurumunuzdaki diđer kiřilere atamanıza imkan tanır. Kullanıcıları destekleyerek Azure AD'de kendi güvenlik gruplarını oluşturup yönetmelerine imkan sağlayabilirsiniz. Grup sahipleri üyelik isteklerini onaylayabilir veya reddedebilir ya da grup üyeliđi denetimini atayabilir.

[Kendi kendini yöneten gruplar oluşturun >](#)

Self servis, kullanıcıları da kapsar. Doğrulanmış bir e-postası olan kullanıcılar self servis portalı aracılığıyla bir hesap için kaydolabilir ve portalı kullanarak parolalarını sıfırlayabilir. Bu, yardım masanızın zamandan ve paradan önemli ölçüde tasarruf etmesini sağlayabilir.

[Self servis parola sıfırlamasını yapılandırın >](#)



Kimlik doğrulamasını modernleştirin

Azure Directory Federasyon Hizmetleri (AD FS) gibi bir şirket içi kimlik doğrulaması kullanıyorsanız uygulamalarınızı Azure AD'ye geçirmeyi düşünebilirsiniz. SSO gibi kullanıcı avantajlarına hala sahip olabilirsiniz, fakat bulutun sunduđu ölçeklenebilirlik ve güvenlik avantajlarını (Azure AD Koşullu Eriřim'i kullanarak ya da Azure AD B2B işbirliđi ile iş ortaklarına kaynak erişimi vererek uygulama başına ayrıntılı erişim denetimi uygulamak gibi) elde edebilirsiniz. Şirket dışında oturum açma için SAML 2.0, WS-Federation, OAuth veya OpenID Connect standartlarını kullanan tüm uygulamalar, geçirilebilir.

[Uygulamalarınıza erişimi güvenli hale getirmek için Azure AD Koşullu Eriřim ilkeleri oluşturun >](#)

[Dış iş ortaklarınızla sorunsuzca işbirliđi yapmak için Azure AD B2B'den yararlanın >](#)

Tüm bulutlardaki veya sunuculardaki tüm uygulamaları güvenli bir şekilde Azure AD'ye bağlayın.

1 milyon bağlı, aktif ve benzersiz uygulama.



Bugün kullanmaya başlayın.

[Bir aylık Azure AD ücretsiz deneme sürümünü](#) başlatarak tüm uygulamalarınıza kullanıcı erişimini yönetmenin ve kurumunuzun güvenliğini sağlamanın ne kadar kolay olduğunu öğrenin.

