

Bulut IAM Kimlik ve Eriřim Yönetimi Platformu

Ürünlerimiz > Bilgi Güvenliđi

Bulut IAM, Türkiye pazarı için özel olarak geliştirilmiş, bulut tabanlı bir Kimlik ve Eriřim Yönetimi (IAM / IDM) hizmetidir. Amacı, işletmenin kimlik ekosistemlerini (çalışanlar, müşteriler, iş ortakları) tek bir platformda güvenle yönetmelerini sağlamaktır.

Bulut IAM, kullanıcılarınız için tüm uygulamalara Tek Oturum (SSO) ile kolayca erişim imkanı sunarken, Çok Faktörlü Kimlik Doğrulama (MFA) gibi gelişmiş güvenlik katmanlarıyla yetkisiz erişimleri engeller. Aynı zamanda, işe başlama ve ayrılma esnasındaki yetkilendirme süreçlerini otomatikleştirir. Bulut IAM kullanıcıların kendi şifrelerini sıfırlamasına olanak tanır ve KVKK gibi yasal düzenlemelere 100% uyum sağlar.



Tüm Kimliklerinizi Güvenle Yönetin

Günümüzün rekabetçi ve hızla dijitalleşen pazarında, işletmenizin en değerli varlıkları olan verilerinizi ve uygulamalarınızı korurken aynı zamanda kusursuz bir kullanıcı deneyimi sunmak, başarının temel taşıdır. Ancak bu dengeyi kurmak, birbirinden kopuk sistemler, artan siber tehditler ve karmaşık yasal düzenlemeler arasında giderek zorlaşmaktadır. İşletmeler genellikle çalışanlarının kimliklerini yönetmek için ayrı, müşterilerinin kimliklerini yönetmek için ise tamamen farklı sistemler kullanır. Bu parçalanmış yaklaşım, yalnızca operasyonel verimsizliklere ve yüksek maliyetlere yol açmakla kalmaz, aynı zamanda ciddi güvenlik açıkları ve tutarsız kullanıcı deneyimleri yaratır. **Stratejik bir bakış açısıyla, bu siloları ortadan kaldıran ve tüm kimlik ekosistemini (çalışanlar, müşteriler, iş ortakları, API'ler) tek bir çatı altında toplayan birleşik bir platform, sadece bir teknoloji yükseltmesi değil, aynı zamanda temel bir iş dönüşümüdür.**



Çalışanlarınız, müşterileriniz ve iş ortaklarınız için kesintisiz, güvenli ve KVKK uyumlu erişim sağlayın. Karmaşıklığı azaltın, verimliliđi artırın ve işinizi geleceđe taşıyın.



Bulut IAM Kimlik ve Eriřim Yönetimi Platformu

Ürünlerimiz > Bilgi Güvenliđi

Bu birleşik vizyon, Toplam Sahip Olma Maliyetinizi doğrudan düşürür, güvenlik duruşunu kökten güçlendirir ve işletmeye, örneğın bir müşterinin aynı zamanda bir iş ortağı haline geldiğı karmaşık ilişkileri yönetme çevikliği kazandırır. **Bulut IAM, bu stratejik dönüşümü gerçekleştirmek için tasarlanmış, Türkiye'nin ihtiyaçlarına özel, bulut tabanlı bir kimlik ve erişim yönetimi (IAM) hizmetidir.**

Eski Kimlik Yönetimi Metodları Neden Yetersiz?

Geleneksel veya parçalanmış kimlik yönetimi yaklaşımları, günümüzün dinamik iş ortamında işletmeleri önemli risklerle karşı karşıya bırakmaktadır.



Artan Güvenlik Riskleri: Parola hırsızlığı, karmaşık oltalama (phishing) saldırıları ve fidye yazılımları her zamankinden daha yaygın. Her yeni bulut uygulaması, her yeni uzaktan çalışan ve her yeni dijital hizmet, potansiyel bir saldırı yüzeyi oluşturur. Birbirinden kopuk sistemler, güvenlik politikalarının tutarlı bir şekilde uygulanmasını imkansız hale getirir ve bir çalışanın erişiminin bir sistemde iptal edilirken diğerinde aktif kalması gibi tehlikeli durumlara yol açar. Bu durum, verileriniz için ciddi ve sürekli bir tehdit oluşturuyor.



Uyum ve Mevzuat Karmaşası: Kişisel Verilerin Korunması Kanunu (KVKK) ve Siber Güvenlik Yasası gibi düzenlemeler, kullanıcı verilerinin nasıl toplandığı, işlendiğı ve saklandığı konusunda katı kurallar getirmektedir. Kullanıcı rızalarını, veri erişim izinlerini ve silme taleplerini manuel olarak veya birden fazla sisteme dağılmış şekilde yönetmek, hem insan hatasına açık, son derece zaman alıcı bir süreçtir hem de ciddi yasal ve finansal risklerle doludur. Olası bir denetimde, tüm bu süreçleri eksiksiz ve tutarlı bir şekilde raporlayabilir misiniz?



Kötü Kullanıcı Deneyimi: Müşterilerinizin her hizmette ayrı hesap ve şifreyle uğraşmak zorunda kalması, müşteri deneyimini olumsuz bir şekilde etkiler. Bu sürtünme, kayıt formlarının yarım bırakılmasına ve doğrudan müşteri kaybına (churn) yol açar. Benzer şekilde, çalışanlarınız her gün kullandıkları onlarca farklı uygulamaya erişmek için sayısız parola ile boğuşmaktan verimlilik kaybeder. Bu durum, genel üretkenliği düşürür ve çalışan memnuniyetsizliğine neden olur.



Yüksek Operasyonel Maliyetler: BT ve yardım masası ekiplerinizin zamanının ne kadarı parola sıfırlama talepleri, kilitlenmiş hesapları açma ve yeni çalışanlar için manuel olarak erişim hakları tanımlama gibi tekrarlayan görevlerle geçiyor? Bu, işletmenizin en değerli teknik kaynaklarının inovasyon, stratejik projeler ve iş geliştirmeye odaklanmak yerine, düşük değerli ve otomatize edilebilir görevlerle meşgul edilmesi anlamına gelir. Bu gizli maliyet, rekabet gücünüzü doğrudan etkiler.



Bulut IAM Kimlik ve Eriřim Yönetimi Platformu

Ürünlerimiz > Bilgi Güvenliđi

Bulut IAM Özellikleri

Bulut IAM, hem iş gücünüzün (Workforce IAM) hem de müşterilerinizin (Customer IAM - CIAM) kimlik yönetimi ihtiyaçlarını tek ve güçlü bir platformda birleştirir. **Platformun her bir özelliđi, belirli bir iş problemini çözmek ve somut bir fayda sağlamak üzere tasarlanmıştır.**



Tek Oturum Açma (Single Sign-On / SSO)

Kullanıcılarınıza, tek bir güçlü kimlik bilgisi seti ile tüm bulut (SaaS) ve şirket içi (on-premise) uygulamalarınıza anında ve güvenli erişim imkanı sunun. Bulut IAM, kimlik sağlayıcı (Identity Provider) olarak hareket ederek SAML2.0, OAuth2.0 ve OpenIDConnect(OIDC) gibi tüm modern federasyon standartlarıyla tam uyumluluk sağlar. Hatta proxy çözümleriyle eski (legacy) web uygulamalarınız için bile SSO yeteneđi kazandırabilirsiniz.

SAML 2.0

OAuth 2.0

OpenID
Connect



Parolasız ve Sosyal Medya ile Giriř (Passwordless & Social Login)

Müşteri ve çalışan deneyimini, en modern kimlik doğrulama yöntemleriyle zenginleştirin. OpenIAM Authenticator mobil uygulaması üzerinden tek dokunuşla onaylanan anlık bildirimler (push notifications), FIDO2/WebAuthn standartları ile biyometrik (parmak izi, yüz tanıma) veya donanım anahtarlarıyla parolasız giriş ve popüler sosyal medya hesapları (Google, Facebook, LinkedIn, Apple , Github vb.) ile hızlı kayıt ve giriş seçenekleri sunun.

Google

Microsoft

facebook

Linkedin

Apple

GitHub



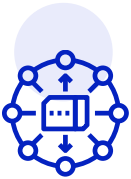
Otomatik Kullanıcı Yönetimi (Automated Provisioning & Deprovisioning)

İnsan kaynakları (İK) sisteminizle (örn. Kolay İK, Odoo, HR Plan, Logo HR, SAP SuccessFactors, Workday, Oracle HCM) entegre olarak, işe yeni başlayan bir çalışanın ilk günden itibaren ihtiyaç duyduğu tüm doğru erişim haklarına (e-posta, CRM, ERP vb.) otomatik olarak sahip olmasını sağlayın. Aynı şekilde, bir çalışan şirketten ayrıldığında, tüm sistemlere olan erişiminin anında ve eksiksiz olarak kesilmesini garanti altına alın. Bu "joiner-mover-leaver" (JML) senaryolarının otomasyonu, manuel işlemleri ortadan kaldırır ve "hayalet kullanıcı" hesaplarından kaynaklanan güvenlik risklerini sıfırlar.



Self-Servis Portal

Kullanıcıları güçlendirerek BT departmanınızın üzerindeki yükü hafifletin. Kullanıcıların kendi parolalarını güvenli bir şekilde sıfırlamalarına, kişisel profil bilgilerini (telefon, adres vb.) güncellemelerine, yeni uygulama erişimleri için talepte bulunmalarına ve onaylanan tüm uygulamalarına tek bir noktadan erişmelerine olanak tanıyan birleşik bir self-servis portalı sunun. Yardım masası taleplerini önemli ölçüde azaltarak BT Destek Yükünü %70'e varan oranda hafifletin ve kullanıcı memnuniyetini artırın.



Modern ve Ölçeklenebilir Mimari

Bulut-yerel (cloud-native) bir platform olarak tasarlanan Bulut IAM, en modern dağıtım teknolojilerini destekler. Docker konteynerları, Kubernetes, Rancher veya OpenShift üzerinde çalışabilen mimarisi sayesinde, işletmeniz büyüdükçe ve kullanıcı sayınız milyonlara ulaştıkça bile performanstan ödün vermeden, esnek ve yüksek kullanılabilirliğe sahip bir şekilde ölçeklenir. Eski ve hantal IAM çözümlerinizi güvenli modernize ederek altyapınızı geleceğe hazırlayın.



Parola Yönetimi

Bu çözümün merkezinde, kullanıcıların yardım masasına başvurmadan kendi parolalarını güvenli bir şekilde sıfırlamalarına olanak tanıyan Kendi Kendine Parola Sıfırlama (SSPR) yer alır. Kullanıcılar, kimliklerini doğrulamak için güvenlik soruları, e-posta veya SMS ile gönderilen tek kullanımlık kodlar veya bir kimlik doğrulama uygulamasından alınan kodlar gibi çeşitli yöntemleri kullanabilirler. Platform, kuruluşların kurumsal standartlara uygun, esnek ve ayrıntılı parola politikaları tanımlamasına olanak tanır. Bu politikalar, parola senkronizasyonu özelliđi sayesinde Active Directory dahil tüm bađlı uygulamalarda tutarlı bir şekilde uygulanır, bu da güvenlik duruşunu güçlendirir ve tutsızlıkları ortadan kaldırır. Zayıf parolaları engellemek için bir "parola sözlüğü", kullanıcıları parolalarının süresi dolmadan önce uyaran proaktif bildirimler ve Windows/MacOS giriş ekranından doğrudan parola sıfırlama gibi özellikler, hem güvenliđi artırır hem de kesintisiz bir kullanıcı deneyimi sađlar. Bu kapsamlı yaklaşım, parola yönetimini otomatize ederek operasyonel verimlilik sađlar.



Merkezi Rıza Yönetimi (Centralized Consent Management)

KVKK ve Siber Güvenlik Yasası uyumluluđunu bir yük olmaktan çıkarıp, bir güven mekanizmasına dönüřtürün. Kullanıcıların hangi kişisel verilerini (örn. e-posta, telefon numarası) hangi amaçla (örn. pazarlama, bülten) paylaştıklarına dair verdikleri rızaları merkezi bir platformda yönetin, sürümleyin ve denetleyin. Kullanıcılara, verdikleri rızaları diledikleri zaman self-servis portalı üzerinden görme ve geri çekme imkanı sunarak tam bir şeffaflık sađlayın.



Kimlik Doğrulama ve Sahtekarlıđı Önleme (Identity Proofing & Fraud Prevention)

Özellikle yeni müşteri kayıt süreçlerinde veya yüksek deđerli işlemlerde, kullanıcıların iddia ettikleri kişi olduklarından emin olun. Üçüncü parti kimlik doğrulama servisleriyle (örn. MERNİS entegrasyonları, e-Devlet doğrulamaları) entegre olarak kullanıcı kimliđini doğrulayın. Bu, sahte hesapların oluşturulmasını, hesap ele geçirme girişimlerini ve diđer dolandırıcılık türlerini proaktif olarak engellemenize olanak tanır.



Görevler Ayrılıđı (Segregation of Duties - SoD)

Tek bir kiřinin bir iřlemi kötüye kullanmasına olanak tanıyan çeliřkili yetkilere sahip olmasını engelleyerek dolandırıcılık ve hata riskini azaltan temel bir güvenlik kontrolüdür. Bulut IAM platformu, bu tür SoD politikalarını merkezi olarak tanımlamanıza ve tüm uygulamalarınızda zorunlu kılmanıza olanak tanır. Sistem, kullanıcı yetkilerini sürekli olarak izler ve bir kural ihlali tespit ettiđinde (örneğin, bir kullanıcıya çeliřkili bir rol atandıđında) uyarı verir ve düzeltici iřlem başlatır. Bu proaktif yaklařım, iç suistimalleri önlemek için kritik bir savunma katmanı sađlar ve kurumsal yönetiřimi güçlendirir.



İř Akıřına Dayalı Eriřim Talebi (Workflow-based Access Request)

Kullanıcıların uygulamalara veya yetkilere eriřim istemeleri için yapılandırılmıř, güvenli ve denetlenebilir bir süreç sunar. Bu özellik, eriřim haklarının kontrolsüz verilmesini engelleyerek "en az ayrıcalık" ilkesini güçlendirir. Kullanıcılar, bir "Hizmet Katalođu" üzerinden ihtiyaç duydukları eriřimi seçer ve talep, yöneticiler veya sistem sahipleri gibi kiřileri içeren önceden tanımlanmıř, çok seviyeli onay iř akıřlarına otomatik olarak yönlendirilir. Onaylayanlar, bu talepleri self-servis portalı, e-posta veya Microsoft Teams gibi kanallar üzerinden kolayca yönetebilir. Bu sistem, kimin, hangi yetkiye, ne zaman ve kimin onayıyla eriřim sađladığına dair eksiksiz bir diđital iz bırakır. Ayrıca, hassas yetkiler için zaman sınırlı eriřim gibi geliřmiř kontroller sunarak güvenlik duruşunu güçlendirir ve yasal uyumluluk denetimleri için raporlamayı kolaylařtırır.



Geliřtirici Dostu REST API

Kapsamlı ve iyi belgelenmiř REST API'miz ile kimlik ve eriřim yönetimi hizmetlerini doğrudan kendi özel web ve mobil uygulamalarınıza, diđital ürünlerinize ve iř akıřlarınıza gömün. Bu, kimlik fonksiyonlarını uygulamanızın ayrılmaz bir parçası haline getirmenize olanak tanır ve geliřtirme ekiplerinize muazzam bir esneklik sunar. Bu, IAM'i bir güvenlik aracı olmaktan çıkarıp, yeni gelir akıřları ve diđital hizmetler yaratmak için bir inovasyon aracına dönüřtürür.

Bulut IAM Kimlik ve Eriřim Yönetimi Platformu

Ürünlerimiz > Bilgi Güvenliđi

Personel Kimlik Yönetimi Deneyimi



Akıllı ve Güvenli Eriřim: Evden çalışan bir pazarlama uzmanı, hassas müşteri verilerini içeren bir rapora erişmek istediğinde, Bulut IAM bu durumu standart dışı bir davranış olarak algılar. Çünkü istek, bilinen şirket IP aralığı dışından gelmektedir. Sistem, kullanıcının parolasını girmiş olmasına rağmen, ek bir güvenlik katmanı olarak pazarlama uzmanının telefonundaki OpenIAM Authenticator uygulamasına bir anlık bildirim (push notification) gönderir. Uzman, bildirimi onaylayarak kimliğini doğrular ve rapora güvenli bir şekilde erişir. Bu süreç, güvenliği en üst düzeye çıkarırken kullanıcı için son derece basittir.



Otomatik İşe Başlatma: İnsan Kaynakları departmanı, yeni bir yazılımcıyı İK sistemine eklediği anda, Bulut IAM'in otomasyon iş akışı tetiklenir. Yazılımcının rolüne ve departmanına göre önceden tanımlanmış olan tüm erişim hakları (Jira, Slack, Office 365, özel geliştirme ortamları, kod depoları) otomatik olarak oluşturulur. Yazılımcı, ilk gününde hiçbir gecikme yaşamadan ve BT ekibine talep açmadan üretken olmaya başlayabilir.



Anında Eriřim İptali: Bir çalışan şirketten ayrılma kararı aldığı anda, İK yöneticisi sistemdeki statüsünü "ayrıldı" olarak günceller. Bu tek bir değişiklik, Bulut IAM'in tüm bağlı sistemlerdeki (bulut ve şirket içi) kullanıcı hesabını ve erişim haklarını anında ve eksiksiz olarak iptal etmesini tetikler. Bu sayede, eski çalışanların hassas şirket verilerine erişme riski tamamen ortadan kalkar.

Müşteri Kimlik Yönetimi Deneyimi



Saniyeler İçinde Kayıt: Yeni bir müşteri, platforma geldiğinde uzun kayıt formları ve karmaşık parola oluşturma kurallarıyla karşılaşmaz. Bunun yerine, "Google ile Devam Et" veya "Facebook ile Giriş Yap" butonlarından birine tıklar. Bulut IAM, sosyal medya sağlayıcısı ile güvenli bir şekilde iletişim kurarak gerekli temel bilgileri alır ve saniyeler içinde müşteri hesabını oluşturur.

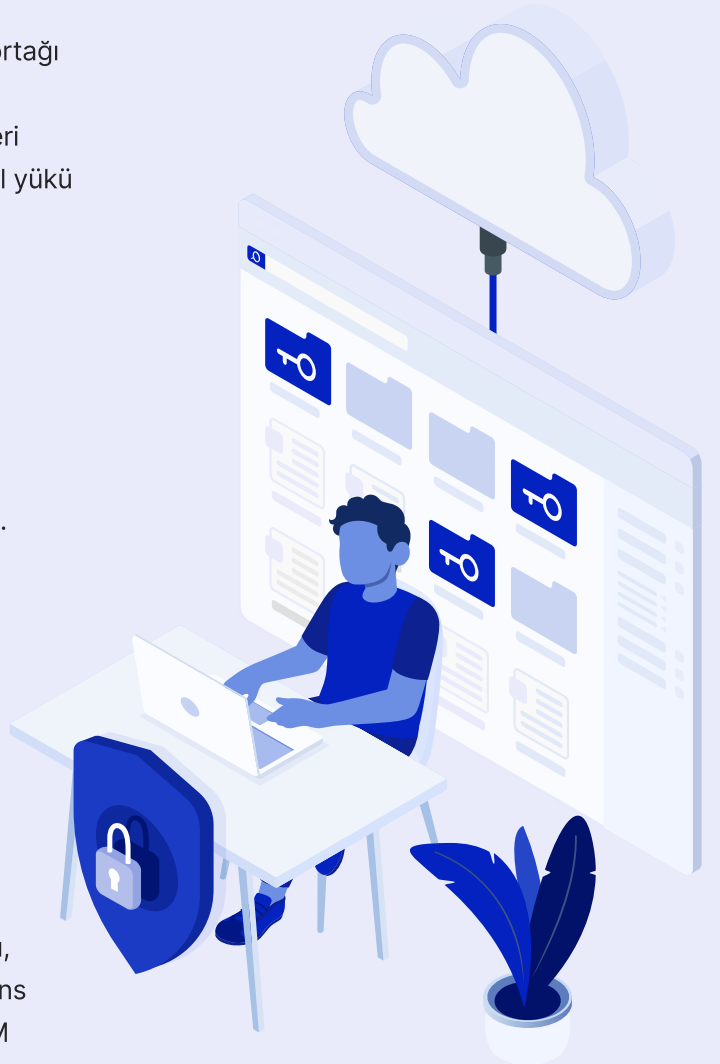
Bulut IAM Kimlik ve Eriřim Yönetimi Platformu

Ürünlerimiz > Bilgi Güvenliđi

- ✓ **Şeffaflık ve Güven:** Müşteri, hesabını oluşturduktan sonra, "Hesabım" bölümündeki self-servis portalına yönlendirilir. Burada, kişisel bilgilerini kolayca güncelleyebilir ve en önemlisi, KVKK kapsamında hangi pazarlama iletişimlerine (e-posta, SMS) izin verdiğini net bir şekilde görebilir ve bu izinleri tek bir tıklama ile yönetebilir. Bu şeffaflık, müşterinin platforma ve markaya olan güvenini artırır.
- ✓ **Kesintisiz Çok Kanallı Deneyim:** Müşteri, web sitesinde bir ürünü sepetine ekledikten sonra, mobil uygulamayı açtığında tekrar giriş yapmasına gerek kalmaz. Bulut IAM'in sağladığı Tek Oturum Açma (SSO) yeteneđi sayesinde, oturumu cihazlar arasında sorunsuzca devam eder.1 Bu kesintisiz deneyim, alışverişin yarım kalmasını engeller ve müşteri memnuniyetini en üst düzeye çıkarır.

Neden Bulut IAM ?

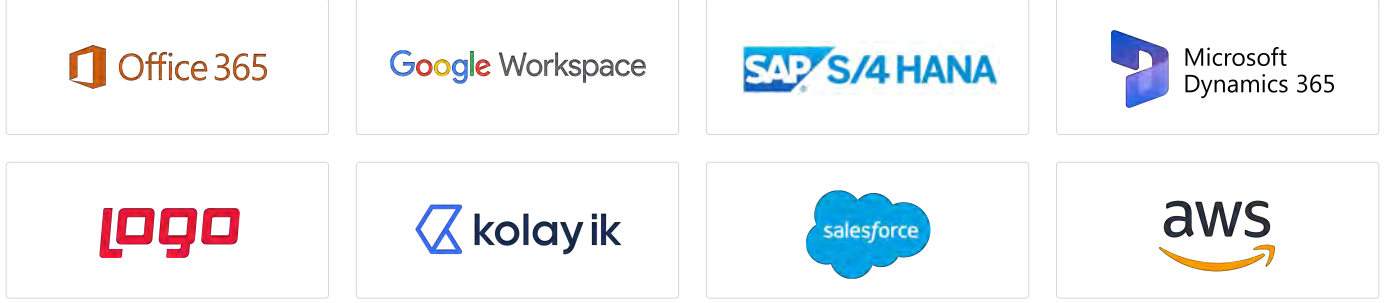
- ✓ **Tek ve Birleşik Platform:** Çalışan, müşteri, iş ortađı ve API kimlikleri dahil tüm kimlik yönetimi ihtiyaçlarınız için tek bir çözüm. Farklı sistemleri yönetmenin getirdiđi karmaşıklık, operasyonel yükü ve maliyetleri ortadan kaldırın.
- ✓ **Derinlemesine Özelleştirme:** Platformumuzu, işletmenizin marka kimliğine, benzersiz iş kurallarınıza ve karmaşık iş akışlarınıza tam olarak uyacak şekilde özelleştirin.1 Kullanıcı kayıt formlarından onay süreçlerine kadar her adımı, sizin iş yapış şeklinize göre şekillendirin.
- ✓ **Yerel Destek ve Uzmanlık:** En büyük farkımız, yerel varlığımızdır. Karşınızda saat farkı olan bir çağrı merkezi deđil, Türkiye'deki ekibimizle, işinizi, pazarınızı ve KVKK gibi yasal gereksinimlerinizi derinlemesine anlayan uzmanlardan doğrudan destek alın.
- ✓ **Maliyet Etkinliđi:** Global rakiplerin karmaşıklığı, uzun implementasyon süreçleri ve yüksek lisans maliyetleri olmadan, kurumsal düzeyde bir IAM platformunun tüm gücüne ve esnekliğine sahip olun. Açık kaynak temelimiz, size daha adil ve şeffaf bir fiyatlandırma sunmamızı sağlar.



Bulut IAM Kimlik ve Eriřim Yönetimi Platformu

Ürünlerimiz > Bilgi Güvenliđi

Bulut IAM Kullanıma Hazır Kütüphaneleri



Bulut IAM'in Bağlayıcı Kütüphaneleri (Connector), platformun işletmenizin kullandığı diğer tüm şirket içi (on-premise) ve bulut tabanlı (SaaS) uygulamalarla sorunsuz bir şekilde iletişim kurmasını sağlayan kritik bir entegrasyon katmanıdır. **Bu kütüphane, Active Directory, SAP, Office 365, Salesforce ve Google Workspace gibi yüzlerce popüler sisteme önceden yapılandırılmış bağlayıcılar sunar. Bu entegrasyonun temel amacı, kimlik yaşam döngüsü yönetimini (örneğin, işe başlama, pozisyon değıştirme ve işten ayrılma süreçleri) tamamen otomatize etmektir.**

Bir çalışan işe başladığında, bağlayıcılar sayesinde tüm ilgili sistemlerdeki hesapları ve yetkileri otomatik olarak oluşturulur. Benzer şekilde, işten ayrıldığında tüm erişimi anında ve eksiksiz olarak kesilir. Bu, manuel işlemleri ortadan kaldırarak operasyonel maliyetleri düşürür, insan hatası riskini sıfırlar ve "hayalet kullanıcı" hesaplarının neden olduğu güvenlik açıklarını önler. **Ayrıca, platformun sunduğu komut dosyası bağlayıcıları ve Yazılım Geliştirme Kiti (SDK), işletmenize özel veya eski sistemler için bile hızlıca yeni entegrasyonlar oluşturma esnekliđi tanır. Bu sayede Bulut IAM, tüm BT altyapınız için merkezi bir kontrol ve otomasyon noktası haline gelir.**

