Delinea

# Bulut Altyapısı Yetki Yönetimi (CIEM)

## Alıcı Kılavuzu

# Bulut Altyapısı Yetki Yönetimi (CIEM) Alıcı Kılavuzu

Bulut dönüşümünün bir sonucu olarak hassas veriler artık firmanın geneline dağılmış durumdadır. Bulut hizmetleri, çoğu zaman merkezi BT denetiminin dışında olmak üzere, hızla oluşturulur. Üstelik hemen hemen bütün firmalar, genellikle veri merkezlerine ve birden fazla Bulut Hizmeti Sağlayıcısına (CSP) yayılmış, tesiste ve bulutta barındırılan kaynakların bir kombinasyonuna sahiptir. Ne yazık ki yanlış yapılandırmalar yaygındır ve bu da kimlikleri güvenlik ihlaline açık hâle getirir veya gereğinden fazla erişim sağlayarak hassas bilgilerin açığa çıkmasına neden olabilir.

Siber suçlular mevcut durumdan yararlanarak bulut kaynaklarına saldırmaktadır. Bunlar çoğunlukla doğrulanmış kimlikleri taklit edip izinlerden faydalanarak erişim kazanır ve erişimi yükseltir, kötü niyetli hedeflerine ulaşırlar.

Normalde tesiste kullanacağınız stratejilerin aynısını kullanarak bulut kaynaklarınızı bunun gibi kimlik tabanlı saldırılara karşı koruyamazsınız. Bu kadar dağınık, dinamik ve kararsız bir ortamda tek bir kimliğin olası veya fiili saldırı yolunu takip etmek, inanılmaz ölçüde zordur. Geleneksel araçlar (ağ güvenlik duvarları, ortak kurumsal dizin hizmetleri ve statik erişim denetimleri) bulut gerçekliğinde etkili değildir.

Bu nedenle, artan kimlik tabanlı saldırılara yanıt olarak kuruluşlar, sahip olunması gereken bir güvenlik çözümü olarak Bulut Altyapısı Yetki Yönetimini (CIEM) benimsiyor. CIEM, kimlik katmanı genelindeki noktalar arasında bağlantı kurar, siz de böylece kimin neye erişimi olduğunu anlayıp denetleyebilir, davranışlarını izleyebilir ve tehditleri kontrol altına almak için hızla yanıt verebilirsiniz.

Bulut güvenliğinden, bulut mimarisinden veya Kimlik ve Erişim Yönetiminden (IAM) siz sorumluysanız ve CIEM çözümlerinin güvenlik yol haritanıza nasıl uyabileceğini düşünüyorsanız bu kılavuz tam size göre.

Kılavuzdaki bilgiler size aşağıdaki konularda yardımcı olacaktır:

- CIEM'in kullanım durumlarını anlama
- Olası çözümleri değerlendirirken sorulacak soruların bir kontrol listesini sunarak CIEM sağlayıcılarıyla görüşmelere hazırlanırken zamandan tasarruf etme
- Seçenekleri karşılaştırma ve ihtiyaçlarınız için en iyi CIEM çözümünü seçme
- CIEM'i genel kimlik güvenliği stratejiniz bağlamında değerlendirme

# Bulutun kimlik güvenliği üzerindeki etkisi

Bulut ortamında kimlik güvenliğinin yönetimi aşağıdaki nedenlerle çok daha karmaşık hâle gelir:

**Dağıtılmış denetim:** Verilere ve kaynaklara küçük bir yönetici grubu yerine çok sayıda kullanıcı ve sistem erişebilir ve hatta bunlar kimlikler de oluşturabilir.

**Rollerin çoğalması:** Rollerin ve izinlerin sayısında ciddi bir patlama yaşandı. Bu durum da bunların özelleştirilmiş araçlar olmadan yönetilmesini ve anlaşılmasını zorlaştırmaktadır.

**Yanlış yapılandırmalar:** Kimlik yönetimi sistemlerindeki ve/veya bulut kaynaklarındaki yanlış yapılandırılmış gruplar, kasıtlı olmasa da riskler ortaya çıkarır.

**Görünürlük boşlukları:** Farklı kimlik sağlayıcıları, birleştirilmiş uygulamalar/hizmetler ve yerel CSP kullanıcılarından oluşan bir kombinasyon, bir bulut ortamı genelinde kimlik izlemeyi kısıtlar ve davranışların anlaşılmasını sınırlandırır.

**Bulut izinlerinin karmaşıklığı:** Modern bulut ortamları, çok sayıda hizmet genelinde binlerce olası izin barındıran karmaşık izin modellerine sahiptir. Yanlışlıkla gereğinden fazla izinler vermek kolaydır, bu da gereğinden fazla ve riskli izinlere yol açar.

**Ayrıcalık yayılması:** Çok fazla sayıda kimlik, gerekenden daha fazla ayrıcalığa sahiptir, bu da en düşük ayrıcalık ve sıfır güven şeklindeki en iyi uygulamaları ihlal etmektedir.

**Sürekli değişim:** Bulut ortamları, sürekli oluşturulan yeni kimlikler (özellikle makine kimlikleri) ve çok hızlı şekilde sağlanan ve kaldırılan yetkilendirmelerle hızlı değişimlere ev sahipliği yapar. Bulut ortamlarının dinamik yapısı, izin sorunlarının manuel olarak giderilmesini ölçeklenemez hâle getirir.

> CIEM, kimlik katmanı genelindeki noktalar arasında bağlantı kurar, siz de böylece kimin neye erişimi olduğunu anlayıp denetleyebilir, davranışlarını izleyebilir ve tehditleri kontrol altına almak için hızla yanıt verebilirsiniz."

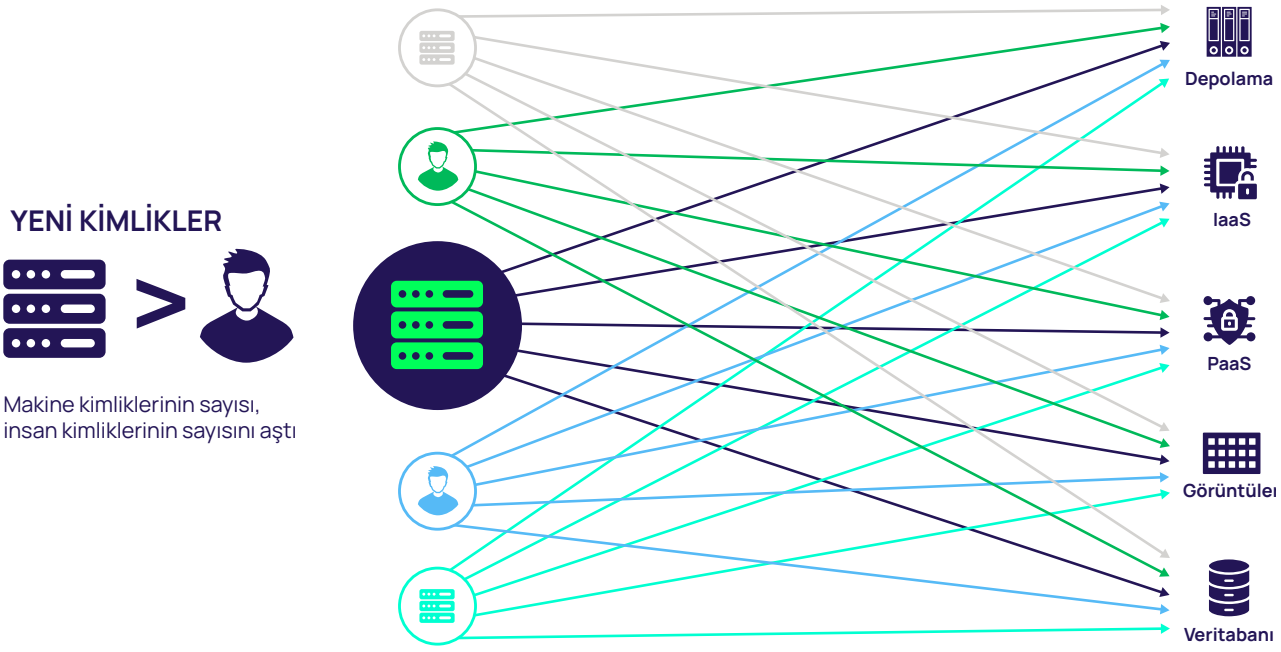
# Bulut Altyapısı Yetki Yönetimi (CIEM)

CIEM, bulut ortamlarında kimlikleri ve bunların ayrıcalıklarını yönetme sürecidir. CIEM'in amacı, bulut ortamlarında ve çok bulutlu ortamlarda hangi erişim yetkilerinin mevcut olduğunu anlamak ve ardından olması gerekenden daha yüksek düzeyde erişim sağlayan yetkilerden kaynaklanan riskleri belirlemek ve azaltmaktır.

CIEM, hibrit ve çok bulutlu ortamlarda hizmet olarak kimlik (IaaS) ve hizmet olarak platform (PaaS) içinde yetkilerin yönetimine yönelik önleyici denetimler uygulayarak bu kimlik tabanlı saldırı risklerini azaltmanıza yardımcı olur. Analiz ve makine öğrenimini (ML) kullanan CIEM, kimlikleri, izinleri ve etkinlikleri sürekli olarak izler. Ayrıcalıkların birikmesi, faal olmayan izinler ve kullanılmayan hesaplar veya roller gibi, hesap yetkilerindeki anormallikleri tespit eder. CIEM, en düşük ayrıcalık ilkesini uygulayarak kimliklerin yalnızca ihtiyaç duydukları unsurlara erişmelerini sağlamaya yardımcı olur ve saldırı yüzeyinizi en aza indirir.

Bulut Tabanlı Uygulama Koruma Platformları (CNAPP) gibi diğer bulut güvenliği çözümlerinin aksine, CIEM çözümleri kimlik riskine odaklanır. CIEM çözümleri ideal olarak, kimlik oluşturma ve yaşam döngüsü yönetim sürecinizin yerleşik bir parçasıdır.

ŞEKİL 1 | Bir bulut hesabındaki kimlik sayısı her bir kimliğin sahip olduğu yetki sayısıyla çarpıldığında, devasa bir saldırı yüzeyi ortaya çıkar.



# CIEM çözümlerinin dört temel kullanımı

## 1 Riskli yetkilere yönelik görünürlük sağlama

CIEM, insanlara ve insan haricinde unsurlara ait kimlikler, hassas varlıklar ve yetkiler için ayrıntılı görünürlük sağlar. BT ortamınızda gezinmek için kullanabilecekleri olası erişim yollarının keşfedilmesi yoluyla size her kimlik için "etkili erişimi" gösterir. Faal olmayan ve gereğinden fazla yetkilerin tespit edilmesi, CIEM çözümlerinde (izin yönetimi veya izin denetimi olarak da bilinir) merkezi bir işlevdir.

## 2 Denetimlerin beklendiği şekilde çalışmasını sağlama

CIEM, kimlik doğrulaması ve yetkilendirme için doğru güvenlik denetimlerinin devreye alınmış ve etkili olduğundan emin olmanıza yardımcı olur. CIEM sayesinde, kimlikle ilgili saldırıların ilk aşamada zemin bulma, erişimi yükseltme veya kalıcılık sağlama olasılığını azaltabilirsiniz.

## 3 Davranış anormalliklerini tespit etme

CIEM, bir siber güvenlik olayı meydana geldiğinde bu durumu anlamanıza yardımcı olur. Kimlikleri ve bunların davranışlarını sürekli izleyerek ve bu bilgilerin anlaşılması için gerekli bağlamı sağlayarak anlamlı veriler toplar. Makine öğrenimi, geçmiş kimlik analizini davranışsal verilerle zenginleştirerek verilen yetkilerin gerçek ihtiyaç ve kullanımla uyumlu olmasını sağlar.

## 4 Kimlikle ilgili riskleri giderme

Otomatik risk giderme, CIEM çözümünün önemli bir özelliğidir. Risk tespit edildiğinde CIEM bir politika ayarlaması önerir veya bir iş akışını tetikler. Örneğin CIEM, faal olmayan ayrıcalıkları kaldırarak gereğinden fazla yetkilendirmeleri ele alabilir, ayrıcalıkları azaltarak politika sapmasını düzeltebilir ve yanlış yapılandırmaları giderme eylemlerini tetikleyebilir.

Bir sonraki bölümde, satıcı değerlendirmenizin bir parçası olarak bu kullanım durumlarının her biri hakkında dilediğiniz CIEM çözüm sağlayıcısına sorabileceğiniz soruları bulacaksınız.

# CIEM çözümü sağlayıcılarına yönelik sorular

## 1. Riskli yetkilere yönelik görünürlük sağlama

Kimlik sağlayıcınız (IdP), CSP'lerinizdeki yetkileri gerçek anlamda anlayamaz. Normal ayrıcalık yayılımı, IdP'niz dışında oluşturulan kullanıcılar (yani yerel yöneticiler veya harici kimlikler tarafından oluşturulanlar), görünmeyen grup üyeliği aracılığıyla verilen ayrıcalıklar ve diğer faktörler, kör noktalar oluşturur. CIEM, fiili durum ve ayrıcalıkların kullanımına ilişkin eksik bilgileri doldurur.

Bu CIEM özellikleri, kimlik saldırısı yüzeyiniz için uçtan uca görünürlük sağlayarak siber güvenlik eylemlerinizin temelini oluşturur.

| CIEM özelliği | Bir CIEM sağlayıcısına sorulacak sorular |
|---|---|
| **İnsan kimliklerini keşfetme** | Birden fazla IdP'yi (Okta, Azure Active Directory, PingOne vb.) destekliyor musunuz?<br>Birleştirme-Taşınma-Ayrılma (JML) değişikliklerini ve kısmi ayrılmayı takip etmek için İK sistemlerine bağlanabiliyor musunuz? |
| **Makine kimliklerini keşfetme** | API'ler ve iş yükleri gibi makine kimliklerini keşfedebiliyor musunuz? |
| **Birleştirilmiş kimlikleri keşfetme** | Harici olarak oluşturulan ve belirteç (token) değişimi yoluyla IdP'nize katılan birleştirilmiş kimlikleri keşfedebiliyor musunuz?<br>AWS'deki etkinliği birleştirilmiş kullanıcılara bağlayıp bunları takip edebilmemi sağlayabiliyor musunuz? |
| **Tüm kritik bulut hizmetlerini, uygulamalarını ve bunların mevcut durumlarını keşfetme** | IaaS ve PaaS, kapsamınıza dahil mi?<br>Hangi CSP'leri destekliyorsunuz?<br>Herkese açık olan hassas klasörleri tespit edebiliyor musunuz?<br>Peki kurum içinde oluşturulan sistemlerimiz için durum nedir? |
| **Tüm kimlik türleri için izinleri ve ayrıcalıkları keşfetme** | Hangi izinlerin kime ve nasıl verildiğini merkezi bir görünümle gösterebiliyor musunuz?<br>Erişim izinleri için dosya düzeyinde ayrıntılı görünürlük sağlayabiliyor musunuz?<br>Gereğinden fazla ayrıcalığa sahip insan ve makine kimliklerini tespit edebiliyor musunuz?<br>Gruplar, ayrıcalık yükseltme yolları ve yanlış yapılandırmalar yoluyla verilen gizli ayrıcalıkları nasıl keşfediyorsunuz?<br>Kendi kimlikleriyle varlıklara erişim imkanına sahip olan yüklenicileri bana gösterebiliyor musunuz? |
| **Kimlikleri birleştirme** | IdP'mizde olmayan ancak varlıklarımıza erişimi olan kimlikler de dahil olmak üzere kimlikleri birleştirebiliyor musunuz? |
| **Sürekli keşfetme** | Sistem, hızlı bir şekilde yönetim altına alınabilmeleri amacıyla, yeni kimlikleri ve varlıkları oluşturulma sürecinde nasıl keşfediyor? |
| **Faal olmayan kimlikleri ve devam eden ayrıcalıkları keşfetme** | Bir kimliğin veya ayrıcalıklı erişimin artık gerekli olmadığını nasıl belirliyorsunuz?<br>Belirtilen dönemler boyunca kullanılmayan ayrıcalıkları tespit ederek erişim ayrıcalığı kullanımını gösterebiliyor musunuz? |

| CIEM özelliği | Bir CIEM sağlayıcısına sorulacak sorular |
|---|---|
| **Ortamlar arasında etkili erişimi keşfetme** | Sistemler ve ortamlar (tesis içi ve çok bulutlu) genelinde erişim yollarını ve yetki izinlerini nasıl takip ediyorsunuz?<br>IdP'den varlığa kadar uçtan uca görünürlük sağlıyor musunuz?<br>Amazon Web Services'ta bana rol zinciri oluşturma, kaynaklara geçici erişim verme gibi ayrıcalık yükseltme yollarını gösterebiliyor musunuz?<br>Hemen kolayca anlaşılabilecek şekilde erişim yollarının görselleştirmelerini nasıl oluşturuyorsunuz? |
| **Risk puanlaması** | Etkili erişime dayalı olarak yüksek riskli kimlikleri tespit edebiliyor musunuz?<br>Toplam erişime dayalı olarak kullanıcılar için risk puanları verebiliyor musunuz?<br>Risk parametrelerini ve tehdit istihbaratını birleşik ve dinamik bir kimlik risk puanı hâlinde bir araya getirebiliyor musunuz? |

## 2. Denetimlerin beklendiği şekilde çalışmasını sağlama

Kimlik tehdidi yüzeyinizi saldırılara karşı korumanın ilk adımı, risklerin bir düşman tarafından kötüye kullanılmadan önce azaltılmasıdır. Kuruluşunuzda halihazırda bazı kimlik denetimleri büyük ihtimalle mevcuttur. Ancak bunların beklendiği gibi işlev gösterdiklerinden ve hiçbir şeyin gözden kaçmadığından emin misiniz?

Bu CIEM özellikleri, kimlik tabanlı bir saldırının zarar yaratabileceği olası kapsamı kontrol altına almak üzere önleyici güvenlik denetimlerinin etkili bir şekilde işlev gösterdiğinden emin olmanıza yardımcı olur. Odaklanılacak öncelikli alanlar, en düşük ayrıcalık ilkesini uygulamak ve ayrıcalık yükseltme yollarını kontrol altına almaktır çünkü bunlar, bir kimliğin güvenliği üzerinde tehlike yaratan bir saldırganın hedeflerine ulaşmak için ihtiyaç duyduğu ayrıcalıklara ulaşmasını engeller.

| CIEM özelliği | Bir CIEM sağlayıcısına sorulacak sorular |
|---|---|
| **Kimlik doğrulaması desteği** | Hangi ayrıcalıklı kimliklerde çok faktörlü kimlik doğrulamasının (MFA) etkin olduğunu ve hangi düzeyde etkin olduğunu gösterebiliyor musunuz?<br>Yanlış IAM yapılandırmalarını ortaya çıkarıp düzeltebiliyor musunuz?<br>Düz metin parolalarının sızdırılmasıyla veya bir kullanıcının kimliğine bürünülmesiyle karşılaşmamıza neden olacak riskli yanlış yapılandırmaları tespit edebiliyor musunuz? |
| **Kimlik doğrulaması desteği** | Kullanıcıların grup üyeliği (ör. iç içe geçmiş gruplar, herkese açık gruplar) aracılığıyla varlıklara nasıl erişim elde ettiğini bana gösterebiliyor musunuz?<br>Ayrıcalıklı erişimi nasıl sınırlandırıyorsunuz?<br>Saldırıları kontrol altına almak için ayrıcalık yükseltme yollarını nasıl ortadan kaldırıyorsunuz? |

## 3. Davranış anormalliklerini tespit etme

Ayrıcalık yükseltme yollarını ve olaylarını tespit etmek, karmaşıklık ve yetersiz görünürlük nedeniyle bulutta son derece zorlu bir iş olabilir. CIEM, güvenliği ihlal edilmiş kimlik bilgileriyle ilk erişim elde etme veya saldırganların zaten içeri sızmış olması durumunda ayrıcalıkları yükseltme girişimleri de dahil olmak üzere, devam eden kimlik tabanlı saldırıları ortaya çıkarmanıza yardımcı olur.

| CIEM özelliği | Bir CIEM sağlayıcısına sorulacak sorular |
|---|---|
| **Taktikleri, teknikleri ve prosedürleri (TTP'ler) tespit etme** | MFA bombalama/yorgunluk saldırılarını tespit edebiliyor musunuz?<br>Deneme yanılma saldırılarını tespit edebiliyor musunuz?<br>Bir kimliğe yönelik ilgili saldırıları gösterebilecek şekilde, birden fazla uygulama üzerinde kimlik bilgisi doldurma yönteminin kullanıldığı başarısız oturum açma girişimlerini tespit edebiliyor musunuz?<br>Oturum ele geçirme saldırısını tespit edebiliyor musunuz? |
| **Şüpheli etkinlik** | Yeni ayrıcalıklı kimliklerin ne zaman oluşturulduğunu tespit edebiliyor musunuz?<br>Faal olmayan ancak tekrar aktif hâle gelen hesapları tespit edebiliyor musunuz?<br>Beklenmedik/istenmeyen ayrıcalık artışını veya yükselişini tespit edebiliyor musunuz?<br>Ek IdP'ler veya İK uygulamaları gibi yeni yukarı akışlı kimlik verisi kaynaklarının bağlantısını tespit edebiliyor musunuz?<br>Yeni oluşturulan kötü amaçlı yanlış yapılandırmaları IdP düzeyinde tespit edebiliyor musunuz?<br>Kullanıcıların IdP'mizdeki günlükler üzerinde yaptıkları, etkinliklerini gizlediklerini gösterebilecek değişiklikleri tespit edebiliyor musunuz? |
| **Kullanım izleme** | Normun dışında bir davranış ortaya çıktığında bunu bilebilmemiz için, bir kullanıcının normal yetki kullanımını belirlemek üzere bir temel etkinlik düzeyi sağlayabiliyor musunuz?<br>İzleme sürekli mi? |
| **Esneklik** | Bir sonraki şirket birleşmesi veya şirket alımında yeni IdP'ler ve uygulamalar için mevcut tespit özelliklerimi genişletmeme nasıl yardımcı olacaksınız? Yeni alınan şirket veya bu şirketin kullanıcıları için kapsamı değiştirme veya tespit politikaları ekleme konusundaki esnekliğinizi açıklamanızı rica ediyorum. |

## 4. Risk azaltma ve giderme

Erişim ayrıcalıkları üzerinde yapılan değişikliklere bağlı olarak, işler üzerinde oluşabilecek etki nedeniyle, risk giderme üstlenilmesi zor bir görev olabilir. CIEM, bir kimliğe etkili erişim, ayrıcalıklı davranış ve bir saldırının zarar yaratabileceği olası kapsam gibi faktörlere dayalı olarak, bağlamla birlikte risklerin nasıl azaltılacağına dair eyleme geçirilebilir bilgiler ve öneriler sağlar.

| CIEM özelliği | Bir CIEM sağlayıcısına sorulacak sorular |
|---|---|
| **Doğru boyutlandırma** | Kimliklerin ve izinlerin doğru boyutlandırılması için önerilerde bulunabilir misiniz?<br>Doğru boyutlandırmanın nasıl yapılacağını anlamak için bağlamı nasıl sağlıyorsunuz? |
| **Risk puanlaması** | Etkili erişime dayalı olarak yüksek riskli kimlikleri tespit edebiliyor musunuz?<br>Toplam erişime dayalı olarak kullanıcılar için risk puanları verebiliyor musunuz?<br>Risk parametrelerini ve tehdit istihbaratını birleşik ve dinamik bir kimlik risk puanı hâlinde bir araya getirebiliyor musunuz?<br>Sağladığınız uyarıların risk puanı formüllerini ayarlayabiliyor muyum? |
| **Uyarı** | İzleme, analiz ve uyarılara yönelik olarak, SIEM gibi güvenlik araçlarımla entegrasyonu nasıl sağlıyorsunuz?<br>JIRA veya ServiceNow gibi BT iş akışı sistemlerinde web kancaları gönderebiliyor veya bilet açabiliyor musunuz? |
| **Politika oluşturma** | İzinler veya roller için yeni politikalar oluşturabiliyor musunuz? |
| **Yeniden düzenleme** | Gerçek kullanıma dayalı olarak, AWS/Azure/GCP izinlerini daha güvenli olacak şekilde otomatik olarak yeniden düzenleyebiliyor musunuz? |
| **Azaltıcı eylemler** | Kimlik bilgileri ele geçirildiğinde, kullanıcıları parolalarını değiştirmeleri yönünde uyarma işlevini otomatikleştirebiliyor musunuz?<br>Çalınan belirteçler (tokens) kullanılarak gerçekleştirilen ele geçirme saldırılarını önlemek için kullanıcıların mevcut oturumlarını otomatik olarak kapatabiliyor musunuz?<br>Kullanıcı şüpheli veya ayrıcalıklı bir etkinlik gerçekleştirdiğinde kendisine ek MFA kullanma zorunluluğu getirebiliyor musunuz? Peki kimlik risk düzeyleri değiştiğinde bunu yapabiliyor musunuz?<br>Üçüncü taraf erişimini kaldırabiliyor musunuz?<br>Koşullu erişimi risk düzeyine göre dinamik olarak ayarlayabiliyor musunuz?<br>Risk giderme iş akışlarını otomatikleştirebiliyor musunuz? |

# İş ortaklığı da önemlidir

Doğru satıcıyı seçmenin önemli bir unsuru, uzun vadeli bir ilişki kuracağınızdan emin olabilmektir. Gerçek bir iş ortağı size yalnızca bir CIEM aracı satmakla kalmamalı, aynı zamanda kimlik güvenliği stratejinizi anlamalı ve hedeflerinize ulaşmanıza yardımcı olmalıdır.

Ancak gerçek şudur ki tek başına CIEM'nin yapabilecekleri, kimlik güvenliği tutumunuzu geliştirmekle sınırlıdır. CIEM'i uçtan uca kimlik yönetimi sürecine dahil etmek, sistemlerin ve ayrıca insanların da birbirleriyle konuştuğu anlamına gelir. CIEM; güvenlik, IAM ve BT operasyonları ekiplerini bir araya getirir çünkü bulutta kimlik ve erişime ilişkin eksiksiz ve doğru bir fikre, ortak bir risk anlayışına ve risk gidermeye yönelik net adımlara sahiptir.

Tüm kimlik ihtiyaçlarınızı anlayan ve beklediğiniz sonuçları zamanında sunabilen bir satıcı arayın. Hoş olmayan sürprizlerden kaçınmak için satıcılara bu soruları önceden sorun.

| Satıcı özelliği | Bir CIEM sağlayıcısına sorulacak sorular |
|---|---|
| **Değer yaratma süresi** | Dağıtım ne kadar sürüyor?<br>1-2 gün içinde işlevsel sonuçları görebiliyor muyum?<br>Olaylara müdahale süresini kısaltmama nasıl yardımcı olacaksınız? |
| **Kullanıma taşınan güvenlik** | Hangi yerel bağlayıcılarınız var?<br>Açık bir API'niz var mı?<br>Çözümünüzü çalıştırmak için komut dosyaları yazmaya gerek var mı?<br>Dağıtım veya entegrasyon için benden ne istiyorsunuz?<br>Güvenlik politikalarını, profesyonel hizmetlere veya yeni özellik geliştirmeye ihtiyaç duymadan riskli hesapları takip edecek ve bunlara ilişkin uyarıda bulunacak şekilde ayarlayabilir miyim?<br>Çözümünüzü, programımızı geliştirirken kullanabileceğimiz diğer ayrıcalıklı hizmetler ve kimlik hizmetleriyle birlikte SaaS platformu üzerinden mi sunuyorsunuz? |
| **Stratejik destek** | Size göre CIEM, genel kimlik güvenliği stratejime nasıl uyuyor?<br>Ekipler arasında uyum oluşturmama nasıl yardımcı olabilirsiniz? |
| **Yanıt verebilme** | Sorularım veya özellik isteklerim olduğunda telefonu açacak mısınız?<br>Teknik belgelerinize erişmek ne kadar kolay?<br>Bana özel atanmış bir başarı yöneticim olacak mı?<br>Yol haritanız hakkında bilgi alabilir miyim? |

# Bulut yetkileri için Delinea öncelik kontrolü hakkında

Bulut yetkileri için Delinea öncelik kontrolü, bulut güvenliği liderlerine bulut ve kimlik kullanımına dair derin bağlam bilgileri sağlayarak çok bulutlu altyapıda riskin azaltılması için gereğinden fazla ayrıcalıkları bulmalarını ve yetkilendirmeyi sınırlamalarını sağlar.

Anormal davranışları belirlemek ve ayrıcalıkları yeniden düzenlemek için tüm kimlikleri, hesapları ve bunların Google, Amazon ve Microsoft bulutlarındaki erişimlerini sürekli olarak bulup görselleştirin. Bulut tabanlı Delinea Platformunda sunulan bulut yetkilerini, tüm kimlikler genelinde yetkilendirme için tek gerçek kaynağınızın bir parçası olarak entegre edebilirsiniz. BT ekiplerini etkilemeden, eski yerel ve birleştirilmiş hesapların bulunması ve geri alınması sürecini otomatikleştirerek zamandan tasarruf edin.

Daha fazlasını öğrenmek için https://delinea.com/products/privilege-control-for-cloud-entitlements bağlantısından web sitemizi ziyaret edin. Bulut yetkileri için Delinea öncelik kontrolünün işleyişini gösteren etkileşimli bir demoyu görün.

Delinea

Securing identities at every interaction

Delinea, merkezi yetkilendirme yoluyla kimliklerin güvenliğini sağlamada öncüdür ve modern kuruluşlar genelinde etkileşimlerini sorunsuz bir şekilde yöneterek kuruluşları daha güvenli hale getirir. Delinea, kurumların kimlikle ilgili tehditleri ortadan kaldırmak için bulut ve geleneksel altyapı, veri ve SaaS uygulamaları genelinde kimlik yaşam döngüsü boyunca bağlam ve zeka uygulamasına olanak tanır. Akıllı yetkilendirme ile Delinea, tüm kimlikleri keşfetmenizi, uygun erişim seviyelerini atamanızı, düzensizlikleri tespit etmenizi ve kimlik tehditlerine gerçek zamanlı olarak anında yanıt vermenizi sağlayan tek platformu sunar. Delinea, aylar değil haftalar içinde devreye girerek ekiplerinizin benimsemesini hızlandırır ve en yakın rakibe göre yönetmek için %90 daha az kaynak gerektirerek onları daha üretken hale getirir. 99,99 çalışma süresi garantisi ile Delinea Platform, mevcut en güvenilir kimlik güvenliği çözümüdür. **LinkedIn**, **Twitter** ve **YouTube**'da Delinea hakkında daha fazla bilgi edinin.