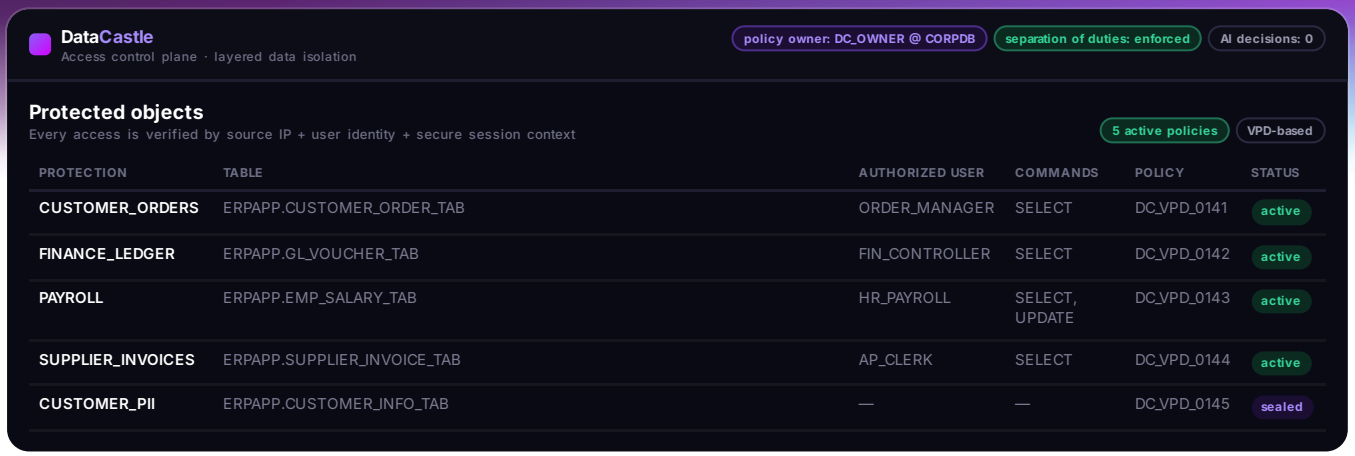
Data Castle

dbo BİLGİ TEKNOLOJİLERİ

AI çağı için tasarlanmış veri güvenliği.

Data Castle, veri tabanı erişimini **ağ katmanından tablo katmanına kadar tek bir mimaride** kapatan bütünleşik bir güvenlik çözümüdür. Her erişim kararı kural tabanlı ve %100 deterministiktir — **çağıran ister bir insan, ister bir uygulama, ister bir AI ajanı olsun.**



Veri tabanınıza artık yalnızca insanlar bağlanmıyor. Güvenlik modeliniz hâlâ öyle varsayıyor.

Veri tabanı güvenliği yıllarca tek bir soruya cevap verecek şekilde kuruldu: bu kullanıcı yetkili mi? **Ama artık bağlantıyı kuran bir copilot, bir entegrasyon ya da bir ajan olabilir — yetkili bir kimlikle ve manipüle edilmiş bir istekle.**

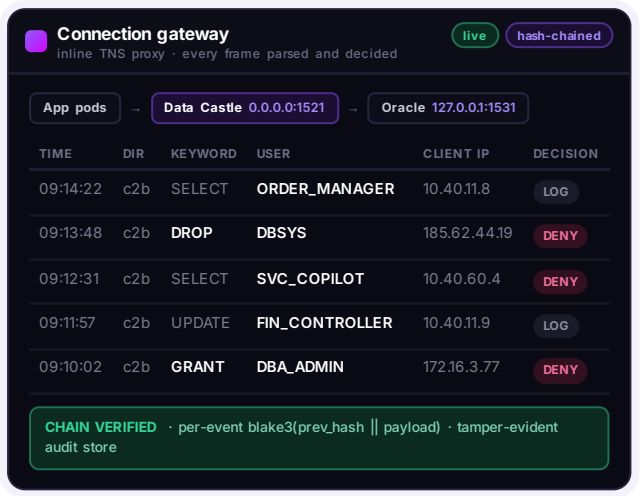
Data Castle kimliğe değil, bağlama güvenir — IP, kullanıcı kimliği ve güvenli oturum bağlamının üçü birden doğrulanmadan hiçbir istemci korunan veriye erişemez. Ele geçirilmiş bir AI ajanı da dahil.

Database Vault, Audit Vault ve Firewall lisanslarına gerek yok.
Mevcut mimarinizi değiştirmenize gerek yok.
Erişim kararlarını bir modele emanet etmenize gerek yok.

ÜRÜN

İlk günden ne değişir.

Data Castle bir Vault taklidi değil, genel amaçlı bir güvenlik katmanı da değil. Korumayı üç katmanda birden kurar: **bağlantı kurulurken, tablo okunurken ve politika değiştirilmek istendiğinde.**

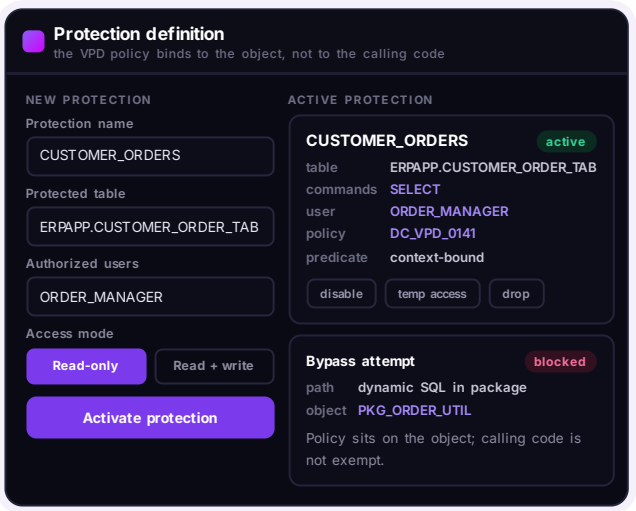


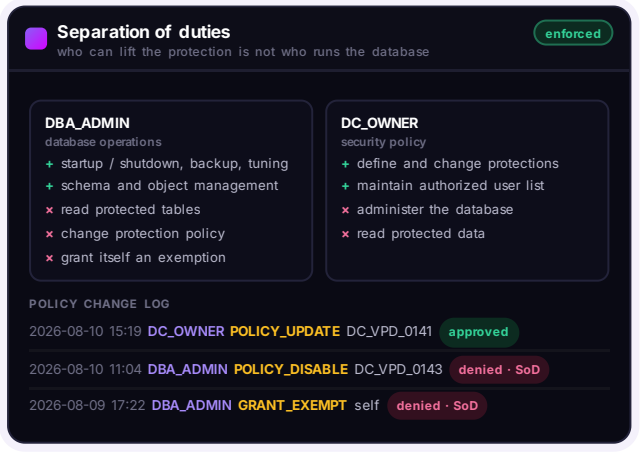
Ağ katmanı: tek kapı

Veri tabanına giden tüm bağlantılar tek bir kapıdan geçer. Uzaktan bağlanan yöneticiler dahil, **sunucu dışından gelen hiçbir erişim bu katmanı atlayamaz.** Trafik gerçek zamanlı izlenir; yetkisiz bağlantılar anında kesilir. Her TNS çerçevesi ayrıştırılır ve her karar **kurcalanamaz bir denetim zincirine** yazılır: her olay blake3 ile öncekine bağlanır, zincir bütünlüğü tek komutla doğrulanabilir.

Tablo katmanı: üç koşul birlikte

Korunan tablolara erişim IP, kullanıcı kimliği ve güvenli oturum bağlamının **üçünün birden** doğrulanmasına bağlıdır. Koruma, Enterprise Edition'ın standart **VPD altyapısı** üzerine kurulur ve politika nesnenin kendisine bağlanır — çağıran koda değil. Bu yüzden paket, prosedür veya dinamik SQL üzerinden de atlatılamaz.





Sökülemezlik katmanı: görevler ayrılığı

Korumayı devre dışı bırakabilecek yetkiler — muafiyet yetkileri dahil — veri tabanını yöneten DBA'lardan ayrı tutulur. Günlük yönetimi yapan kimlik ile güvenlik politikasını değiştirebilecek kimlik **asla aynı değildir.** Güçlü bir yönetici hesabı ele geçirilse bile koruma kuralı üzerinde tek başına oynama yapılamaz.

MİMARİNİN DEĞİŞMEZLERİ

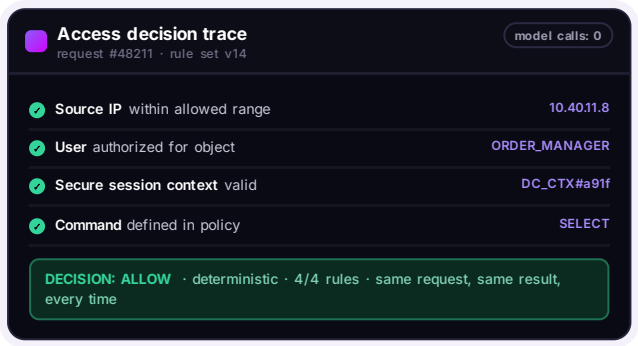
3	%100	0	0
koruma katmanı: ağ, tablo, sökülemezlik	deterministik erişim kararı — tahmin yok, model yok	atlatma yolu: paket, prosedür ve dinamik SQL dahil	ayrıca lisanslanan Vault ve Firewall bağımlılığı

info@dbotech.uk

AI ÇAĞINA KARŞI TASARLANDI

Çağıranın kim olduğu önemsizdir.

Veri tabanlarına giderek daha fazla AI ajanı ve copilot entegrasyonu erişiyor. Bu, yeni bir saldırı yüzeyi demek: prompt injection, aşırı yetkilendirilmiş AI erişimi, modelin manipüle edilerek yetkisiz veri çekmeye yönlendirilmesi. Data Castle bu riske iki yönden kapalıdır.

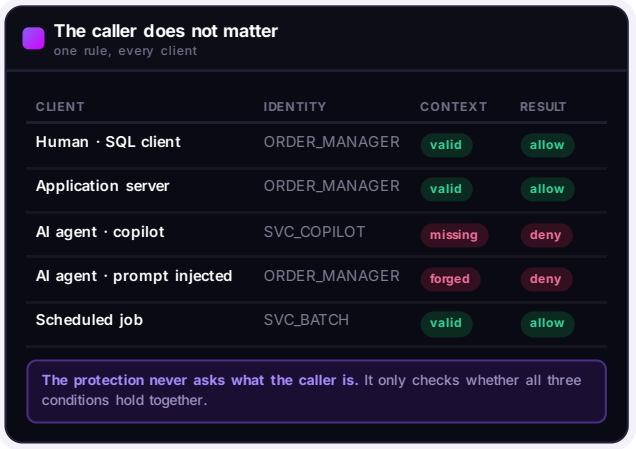


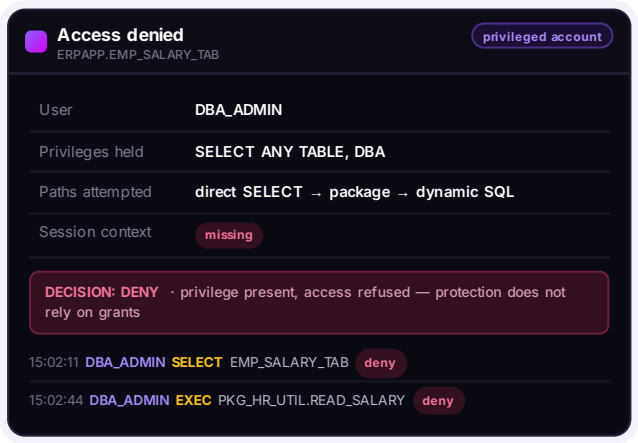
Karar katmanında yapay zekâ yok

Erişim kararları hiçbir yapay zekâ modeline veya olasılıksal tahmine dayanmaz. Kural tabanlı, %100 deterministik ve tekrarlanabilirdir; aynı istek her seferinde aynı sonucu verir. Bu da denetim karşısında — **BDDK ve SPK dahil — tam savunulabilirlik** sağlar. Güvenlik ürününüzün kendisi bir kara kutu değildir. Denetçinin isteyeceği raporlar BDDK, KVKK ve PCI DSS madde eşlemeleriyle hazır gelir.

İstemciye güven yok

Koruma, bağlantıyı yapan yazılımın bir insan mı, bir uygulama mı, yoksa bir AI ajanı mı olduğuna güvenmez. IP, kullanıcı kimliği ve oturum bağlamı doğrulanmadan hiçbir istemci korunan veriye erişemez. **Ele geçirilmiş veya manipüle edilmiş bir ajan da bu kuralın dışında değildir.**





Yönetici yetkisi bloklama

Ayrıcalıklı ve paylaşılan kullanıcıların — **DBA dahil** — korunan tablolara erişimi veri tabanı seviyesinde engellenir. AI entegrasyonları çoğu zaman geniş yetkili servis hesaplarıyla çalışır; Data Castle ile bu hesapların yetkisi artık veriye erişim garantisi değildir.

DENETİME HAZIR RAPORLAMA

BDDK
Md.5 / Md.7 / Md.12 / Md.15 eşlemeli olay özetleri ve kimlikleri

KVKK
Md.4 / Md.5 / Md.7 ve silinme hakkı; veri maskeleme bulguları

PCI DSS v4
10.2.1 / 10.2.2 / 10.2.4 / 10.2.7 audit log gereksinimleri

Yetkili erişim
DBA, SYS, SYSTEM ve SYSDBA erişimleri ile son aktivite anları

KİMLER İÇİN · VERİNİZİ NASIL KORUYORUZ

Hassas veri tutan her kurulum için. *Mimarinizi değiştirmeden çalışır.*

İş birimleri verinin korunduğunu bilir. Bilgi güvenliği, denetim ve IT ekipleri ise onay verebilmek için gereken belirlenebilirliği, görevler ayrılığını ve iz kaydını alır.

Her ekip için değer

Mevcut mimarinize dokunmadan, ilk günden.
Örnek kullanım alanları:

- **Bilgi güvenliği**
  Ayrıcalıklı hesap riski veri tabanı seviyesinde kapanır; DBA yetkisi artık veriye erişim anlamına gelmez.
- **İç denetim ve uyum**
  Her erişim kararı açık kurallarla verilir ve tekrarlanabilir; BDDK ve SPK dahil denetimlerde savunulabilir.
- **Veri tabanı yönetimi**
  Günlük DBA işleri değişmez; güvenlik politikası ayrı bir kimliğe taşınır, sorumluluk netleşir.
- **Uygulama ekipleri**
  Koruma nesne seviyesinde çalıştığı için uygulama kodu değişmez; ek entegrasyon riski taşımaz.
- **AI ve entegrasyon projeleri**
  Copilot ve ajan entegrasyonları geniş yetkili servis hesaplarıyla çalışsa bile korunan veriye erişemez.
- **Finans ve satın alma**
  Database Vault, Audit Vault ve Firewall lisanslarına gerek duymaz.

Güven ve kontrol

Sizin altyapınız. Sizin kurallarınız. Sizin verileriniz.

- **Üç katmanlı koruma**
  Ağ, tablo ve sökülemezlik katmanları bağımsız çalışır; tüm bağlantılar tek kapıdan geçer, anormal olanlar anında kesilir.
- **Karar katmanında model yok**
  %100 kural tabanlı, deterministik ve tekrarlanabilir. Sonuç tahmin edilebilir.
- **Atlatma yolları kapalı**
  Politika nesneye bağlanır; paket, prosedür ve dinamik SQL denemeleri de aynı kontrole tabidir.
- **Görevler ayrılığı**
  Politikayı değiştirebilecek ve muafiyet alabilecek yetki, veri tabanını yönetenden ayrıdır.
- **Kurcalanamaz denetim izi**
  Her erişim denemesi ve politika değişikliği loglanır ve blake3 ile önceki olaya bağlanır; zincir doğrulanabilir.
- **Standart altyapı üzerinde**
  Enterprise Edition'ın standart VPD işlevi üzerine kurulur; ek lisans gerektirmez.

Ücretsiz
Güvenlik değerlendirmesi

30 dakikalık teknik görüşmeyle başlayın. Mevcut kurulumunuzdaki ayrıcalıklı erişim ve atlatma yollarını birlikte tarayalım. Sonunda **hangi tablolara hangi yollarla erişilebildiğini gösteren bir bulgu raporu** alırsınız.
Maliyet yok. Taahhüt yok.

30 dakikalık görüşme planla →

veya info@dbotech.uk adresine yanıt verin