

SQL Change Guard

Sistem Mimarisi ve Topoloji

Bileşenler, Veri Akışı ve Dağıtım

On-premise | SQL Server | PostgreSQL | Oracle

1. Bileşen Mimarisi

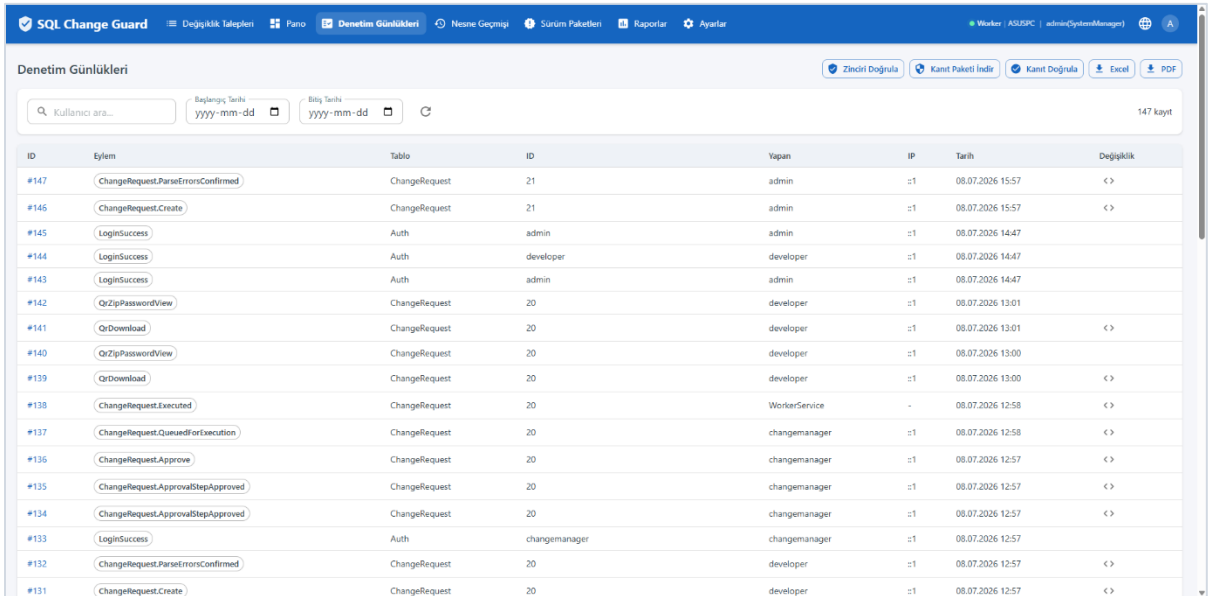
SQL Change Guard üç ana çalışma zamanı bileşeninden oluşur; hepsi kurum ağı içinde çalışır.

- Web Arayüzü (React): kullanıcıların değişiklik ve sorgu taleplerini yönettiği sunum katmanı
- REST API (.NET 10): iş kuralları, yetkilendirme, parse, risk bandı belirleme, policy engine ve audit motorunun bulunduğu çekirdek
- Worker (Windows Service, Quartz): onaylı talep ve paketlerin hedefte çalıştırılması (elle başlatılanlar dahil), zamanlanmış çalıştırma, kanıt sınırı denetimi ve defter özeti gibi arka plan işleri

İş mantığı yalnızca backend'dedir. UI kontrolü tek başına güvenlik olarak kabul edilmez; tüm kurallar API tarafında tekrar doğrulanır.

2. Veri Katmanları

- Uygulama veritabanı (SQL Server 2022 ve sonrası): talepler, scriptler, onaylar, roller, parametreler, policy tanımları, raporlar. Denetim kayıtları evidence şemasındaki append-only defter (ledger) tablosundadır; veritabanı motoru bu tabloda UPDATE ve DELETE işlemlerini reddeder; tabloya yalnız tek bir yazma yordamıyla yazılır
- Defter özeti klasörü: API'nin defter özetlerini (imza açıksa imzalı) yazdığı klasör (Evidence:Ledger:DigestOutputPath). Klasörün değiştirilemez bir depoda (WORM gibi) ve veritabanı yöneticisinin yazamayacağı bir yerde olması kurumun sağlamasıdır
- Hedef veritabanları (SQL Server / PostgreSQL / Oracle): değişikliklerin uygulandığı ve sorguların çalıştığı canlı sistemler



The screenshot displays the 'Denetim Günlükleri' (Audit Logs) section of the SQL Change Guard application. The interface includes a search bar, date filters for 'Başlangıç Tarihi' (Start Date) and 'Bitiş Tarihi' (End Date), and buttons for 'Zinciri Doğrula' (Verify Chain), 'Kanıt Paketi İndir' (Download Evidence Package), 'Kanıt Doğrula' (Verify Evidence), 'Excel', and 'PDF'. The table below lists 147 records, showing details such as ID, Action, Table, ID, User, IP, Date, and Change.

ID	Eylem	Tablo	ID	Yapan	IP	Tarih	Değişiklik
#147	ChangeRequest.ParseErrorsConfirmed	ChangeRequest	21	admin	±1	08.07.2026 15:57	<>
#146	ChangeRequest.Create	ChangeRequest	21	admin	±1	08.07.2026 15:57	<>
#145	LoginSuccess	Auth	admin	admin	±1	08.07.2026 14:47	
#144	LoginSuccess	Auth	developer	developer	±1	08.07.2026 14:47	
#143	LoginSuccess	Auth	admin	admin	±1	08.07.2026 14:47	
#142	QrZipPasswordView	ChangeRequest	20	developer	±1	08.07.2026 13:01	
#141	QrDownload	ChangeRequest	20	developer	±1	08.07.2026 13:01	<>
#140	QrZipPasswordView	ChangeRequest	20	developer	±1	08.07.2026 13:00	
#139	QrDownload	ChangeRequest	20	developer	±1	08.07.2026 13:00	<>
#138	ChangeRequest.Executed	ChangeRequest	20	WorkerService	-	08.07.2026 12:58	<>
#137	ChangeRequest.QueuedForExecution	ChangeRequest	20	changemanager	±1	08.07.2026 12:58	<>
#136	ChangeRequest.Approve	ChangeRequest	20	changemanager	±1	08.07.2026 12:57	<>
#135	ChangeRequest.ApprovalStepApproved	ChangeRequest	20	changemanager	±1	08.07.2026 12:57	<>
#134	ChangeRequest.ApprovalStepApproved	ChangeRequest	20	changemanager	±1	08.07.2026 12:57	<>
#133	LoginSuccess	Auth	changemanager	changemanager	±1	08.07.2026 12:57	
#132	ChangeRequest.ParseErrorsConfirmed	ChangeRequest	20	developer	±1	08.07.2026 12:57	<>
#131	ChangeRequest.Create	ChangeRequest	20	developer	±1	08.07.2026 12:57	<>

Audit Logs - append-only denetim kayıtları

3. Mantıksal Akış (Change)

- 1. Kullanıcı web arayüzünden değişiklik talebi (script) oluşturur
- 2. API script'i parse eder, 88 SQL standardıyla doğrular ve risk bandını (Info, Low, Medium, High, Critical) belirler
- 3. Policy engine sunucu/ortam/tip'e göre onay adımlarını belirler
- 4. Yetkili onaylayıcılar rol bazlı olarak onaylar
- 5. İsteğe bağlı: sandbox'ta çalıştır ve geri al ile ön doğrulama
- 6. Kullanıcı ya da zamanlama çalıştırmayı başlatır; Worker, onaylanan içerikle çalışacak içeriğin aynı olduğunu denetledikten sonra değişikliği hedef veritabanında tek transaction ile çalıştırır (Oracle'da örtük COMMIT yapan ifadeler bu transaction'ın dışında kalır)
- 7. Sonuç ve tüm adımlar kanıt defterine yazılır

4. Mantıksal Akış (Production Query)

- 1. Kullanıcı production sorgu (SELECT) talebi oluşturur
- 2. Onay politikası sunucu, ortam ve talep türüne göre adımları belirler; kolon önizlemesi hassas kolonları teslimden önce gösterir
- 3. Gerekli onaylar alınır (politikadaki adımlar; maskesiz kolon için ek onay, varsayılan onaylayan System Manager)
- 4. Sorgu çalışır; hassas kolonlar maskelenir
- 5. Sonuç şifreli ZIP olarak teslim edilir; indirme gerekçesi ve indirme kaydı tutulur
- 6. Tüm süreç audit ve QR maskeleye günlüğüne yazılır

5. Ağ Topolojisi

Tüm bileşenler kurum ağına konumlanır; internet bağlantısı gerekmez.

- İstemciler → Web/API (HTTPS)
- API ve Worker → Uygulama SQL Server (yönetim verisi)
- API → Defter özeti klasörü (defter özetleri, imza açıksa imzalı; Worker bu klasöre erişmez)
- API / Worker → Hedef veritabanları (SQL Server, PostgreSQL, Oracle)
- API → LDAP/AD ve kurum kimlik sağlayıcısı (OIDC/SAML) (kimlik), SMTP (bildirim) ve ITSM (isteğe bağlı); API ve Worker → SIEM (Syslog ya da dosya, isteğe bağlı); Worker → API (yapılandırma, canlılık ve imza istekleri)

Sunucu Adı	Host	Veritabanı Tipi	Ortam	Aktif	CR Otomatik Çalıştırma	QR Otomatik Çalıştırma	Rollback Zorunlu	İşlemler
ASUSPC	ASUSPC1433	SqServer	Production	✓	-	-	-	
ASUSPC\SQLEXPRESS	ASUSPC\SQLEXPRESS:1433	SqServer	Test	✓	-	-	-	
ASUSPC\SQLEXPRESS01	ASUSPC\SQLEXPRESS01:1433	SqServer	Test	✓	-	-	-	
oracletest	db.freessql.com/23a1_34u2-2404	Oracle	Test	✓	-	-	-	
PostgreSQL_Test	ep-withered-moon-atrag@fc-9-us-east-1.aws.neon.tech:5432	PostgreSQL	Test	✓	-	-	-	

Sunucu Yönetimi - çoklu SQL Server / PostgreSQL / Oracle tek yerden

6. Yüksek Erişilebilirlik ve Kurtarma

- Tek transaction executor: bir talebin tüm adımları tek transaction altında; hata durumunda geri alınır (SS/PG)
- Oracle: DDL, DCL ve TRUNCATE örtük COMMIT yaptığı için bu ifadeler transaction ile geri alınamaz; böyle ifade içeren Oracle değişikliklerinde geri alma planı zorunludur ve otomatik hazırlanabilir. PL/SQL bloklarında transaction izlenir, verinin kalıcı olup olmadığı belirsizse talep uzlaştırmaya alınır
- Denetim kaydı: defter tablosu kayıt değiştirmeyi ve silmeyi reddeder; Worker varsayılan olarak saatte bir özet turunu başlatır, API defter özetini (imza açıksa imzalı) yapılandırılan klasöre yazar
- Uygulama veritabanı standart yedekleme/replikasyon ile korunabilir; özet klasörü kurumun saklama politikasıyla korunur. Eski bir yedeğe dönülmesi ancak dış defter özetiyle karşılaştırmada fark edilir

7. Hedef bağlantı, oturum yoklaması ve pencere olayları

Ürün hedef veritabanına bağlanırken şu üç şeyi bırakır: bir oturum adı, sunucunun söylediği oturum numarası ile istemci adresi ve denetim izinde bir başlangıç ve bir bitiş olayı.

- Bağlantı fabrikası: her hedef bağlantı SQL Change Guard/<Rol>/<Numara> adıyla açılır. Kimlik taşıyan beş rolde (Execute, Query, Release, Sandbox, SandboxRelease) havuz kapalıdır.
- Oturum yoklaması: bağlantı açılınca hedefe tek bir okuma sorgusu atılır; oturum numarası ve hedefin gördüğü istemci adresi alınır. Her veritabanı türü için ayrı yoklayıcı vardır (SQL Server, PostgreSQL, Oracle).
- Pencere kaydedici: Worker, başlangıç olayını bağlantı açıldıktan sonra, hedefte ve uygulama veritabanında işlem başlamadan önce yazar; bitiş olayını iş bitince yazar. Başlangıç yazılamazsa betik çalışmaz.
- API yalnız sandbox isteğini (SandboxRequested) yazar; hedefe iş yapan bağlantılar Worker'dadır. API'nin önizleme, tanım okuma ve bağlantı deneme bağlantıları pencere açmaz.
- Çıkış yolları: denetim izi, Expected Access Principals raporu, denetim dosyası ve SIEM. DAM ile eşleşme bu çıktılar üzerinden yapılır. Ürün DAM değildir: canlı trafiği dinlemez ve ürün dışında yapılan işlemleri engellemez.

8. İletişim

- Web: www.sqlchangepguard.com
- E-posta: onur.egilmez@sqlchangepguard.com | info@sqlchangepguard.com
- Telefon: 0505 621 29 02
- LinkedIn: [linkedin.com/company/sqlchangepguard](https://www.linkedin.com/company/sqlchangepguard)