

BEFORE QENTRA / AFTER QENTRA

Same Application. Same SQL Server.
A Smarter, More Intelligent Data Layer.

Quentra sits between your applications and SQL Server.
Without changing your application code, it analyzes, optimizes,
secures, and protects your SQL traffic in real time.



	BEFORE QENTRA	WHAT QENTRA DOES	AFTER QENTRA
01 IN-FLIGHT QUERY REWRITE Guess. Hope. Optimize SQL.	Legacy or poorly written queries run as is. They consume excessive resources: CPU and I/O are high, response times are slow.  5.2 sec  420K reads	Quentra reaches SQL Server before your queries even get there and automatically optimizes them using intelligent rules. <pre>SELECT * FROM Orders WHERE OrderDate >= '2024-01-01' AND OrderDate < '2025-01-01' AND CustomerID LIKE 'ABC%'</pre> Quentra AI Query Rewrite Engine	✓ No application changes ✓ More logical reads ✓ Lower CPU usage ✓ Much faster response  95 ms  1.8K reads
02 SMART QUERY CACHE Same Question. Don't Ask Again.	Dashboards and frequent users run the same queries again and again on SQL Server.   100 requests → SQL Server	Frequently asked queries are intelligently cached. Only what's needed is sent to SQL Server.    100 requests → QENTRA CACHE → 1 SQL Call	✓ Lower query load ✓ Lower CPU & I/O ✓ Faster applications ✓ Higher user capacity 
03 BRUTE-FORCE PROTECTION Stop Attacks Before They Reach Your Data.	IP addressees can be scanned. Login attempts can be brute-forced. Malicious requests can bring SQL Server down.  1 IP · 60 sec · 847 Login Attempts	Behavior is analyzed in real time. Malicious patterns are detected and blocked instantly.  Quentra Threat Engine	✓ IP-aware protection ✓ Behavioral analysis ✓ Automatic blocking ✓ Safe SQL access  1 IP · 60 sec · 847 Attempts BLOCKED
04 SQL INJECTION PROTECTION Harmful SQL Can Destroy Your Server.	SQL injection attacks can read, modify or delete your data. They can take down your system. <pre>' OR 1=1 --</pre>  SQL Attack Detected	SQL traffic is analyzed in real time. Harmful SQL statements are detected and blocked before they reach SQL Server.  Quentra SQL Firewall	✓ SQL injection detected ✓ Real-time prevention ✓ Data integrity ✓ Unauthorized access blocked  <pre>' OR 1=1 --</pre>BLOCKED
05 DATA SENTINEL Sensitive Data Should Stay Private.	ID: 12345678901 Phone: 0532 123 45 67 Email: omer@example.com Address: İstiklal Cad. No:12 D:5 Sensitive data shown in applications can lead to privacy violations.	Sensitive data is masked in real time based on your policies.  Quentra Data Sentinel	ID: 123*****01 Phone: 0532 *** ** 67 Email: o***@example.com Address: İstiklal Cad. No:** D:** ✓ No application changes ✓ Policy-based masking ✓ Compliance ready ✓ Audit visibility
06 AUDIT KEEPER Who, When, What? Know Everything.	You have no idea who ran what, when, from where. There are no proper logs. No clear answers.   	All SQL traffic is recorded and logged with who, what, when, where, and how. Easy auditing, full visibility.  Quentra Audit Engine	14:32:18 ERP-APP User: reporting_user IP: 10.10.4.21 Action: SELECT Database: ERP Status: ✓ Logged ✓ Complete audit trail ✓ User & app tracking ✓ Incident investigation ✓ SQL visibility

Don't Change Your Application → Change Your SQL Traffic with Quentra

 PERFORMANCE Query Rewrite + Cache Lower CPU Faster SQL Lower Costs	 SECURITY Brute-Force + SQL Injection Stop Attacks Protect Your Data	 DATA PROTECTION Real-Time Masking Protect Sensitive Data Share with Confidence	 VISIBILITY Complete SQL Audit Trail Know Everything Stay in Control
---	---	--	---