

# Data security built for the AI era.

Data Castle is an integrated security solution that closes database access **in one architecture, from the network layer down to the table layer**. Every access decision is rule-based and 100% deterministic — **whether the caller is a human, an application or an AI agent**.

 **DataCastle**  
Access control plane · layered data isolation

policy owner: DC\_OWNER @ CORPDB

separation of duties: enforced

AI decisions: 0

**Protected objects**  
Every access is verified by source IP + user identity + secure session context

5 active policies

VPD-based

| PROTECTION        | TABLE                       | AUTHORIZED USER | COMMANDS          | POLICY      | STATUS |
|-------------------|-----------------------------|-----------------|-------------------|-------------|--------|
| CUSTOMER_ORDERS   | ERPAPP.CUSTOMER_ORDER_TAB   | ORDER_MANAGER   | SELECT            | DC_VPD_0141 | active |
| FINANCE_LEDGER    | ERPAPP.GL_VOUCHER_TAB       | FIN_CONTROLLER  | SELECT            | DC_VPD_0142 | active |
| PAYROLL           | ERPAPP.EMP_SALARY_TAB       | HR_PAYROLL      | SELECT,<br>UPDATE | DC_VPD_0143 | active |
| SUPPLIER_INVOICES | ERPAPP.SUPPLIER_INVOICE_TAB | AP_CLERK        | SELECT            | DC_VPD_0144 | active |
| CUSTOMER_PII      | ERPAPP.CUSTOMER_INFO_TAB    | —               | —                 | DC_VPD_0145 | sealed |

**Your database is no longer reached only by people.  
Your security model still assumes it is.**

For years database security was built to answer a single question: is this user authorized? **But the connection may now be opened by a copilot, an integration or an agent — with an authorized identity and a manipulated request.**

**Data Castle trusts context, not identity** — no client reaches protected data unless source IP, user identity and a secure session context are all verified together. A compromised AI agent included.

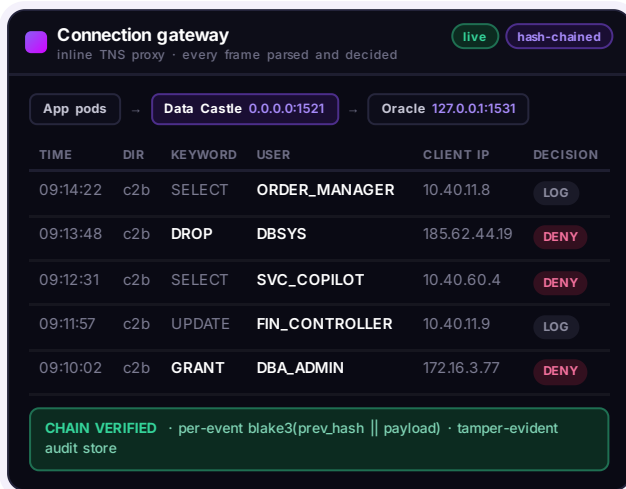
**No Database Vault, Audit Vault or Firewall licence needed.**

**No change to your existing architecture.**

**No access decision left to a model.**

# What changes on day one.

Data Castle is not a Vault imitation, and it is not a general-purpose security layer. It builds protection across three layers at once: **as the connection opens, as the table is read, and when someone tries to change the policy.**

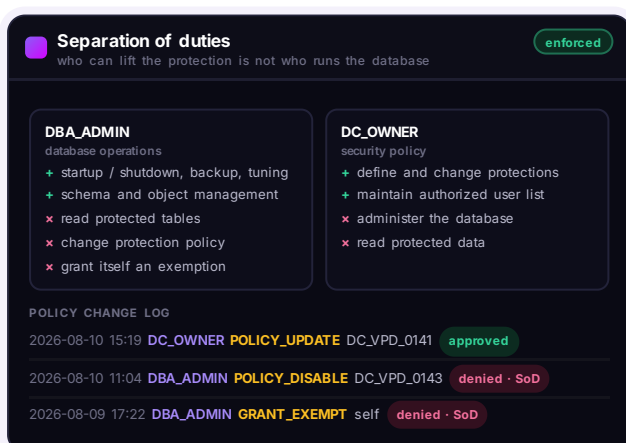
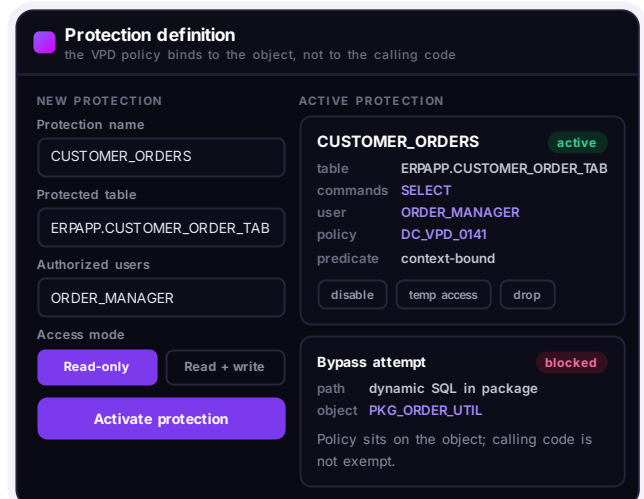


## Network layer: one door

Every connection to the database passes through a single gate. Including administrators connecting remotely, **no off-box access can bypass this layer.** Traffic is monitored in real time and unauthorized connections are cut immediately. Every TNS frame is parsed and every decision written into a **tamper-evident audit chain**: each event is bound to the previous one with blake3, and chain integrity is verifiable with a single command.

## Table layer: three conditions together

Access to protected tables depends on source IP, user identity and a secure session context being verified **all three at once**. Protection is built on the standard **VPD capability** of Enterprise Edition, and the policy binds to the object itself — not to the calling code. That is why it cannot be bypassed through packages, procedures or dynamic SQL.



## Non-removability layer: separation of duties

The privileges that could lift the protection — exemption privileges included — are held apart from the DBAs who run the database. The identity doing daily operations and the identity able to change security policy are **never the same**. Even if a powerful administrator account is compromised, no one can alter the protection rule alone.

### ARCHITECTURAL CONSTANTS

3

protection layers: network, table, non-removability

100%

deterministic access decisions — no guesswork, no model

0

bypass paths: packages, procedures and dynamic SQL included

0

dependency on separately licensed Vault or Firewall

# The caller does not matter.

More AI agents and copilot integrations reach databases every month. That is a new attack surface: prompt injection, over-privileged AI access, a model manipulated into pulling data it should not. Data Castle is closed to this risk from two directions.

Access decision trace

request #48211 · rule set v14

model calls: 0

Source IP

within allowed range

10.40.11.8

User

authorized for object

ORDER\_MANAGER

Secure session context

valid

DC\_CTX#a91f

Command

defined in policy

SELECT

DECISION: ALLOW

· deterministic · 4/4 rules · same request, same result, every time

## No AI in the decision layer

Access decisions rest on no AI model and no probabilistic guess. They are rule-based, 100% deterministic and repeatable; the same request returns the same result every time. That gives you **full defensibility in front of financial regulators and supervisory authorities**. Your security product is not itself a black box, and the extracts an auditor asks for arrive already mapped to their articles.

## No trust in the client

The protection does not trust whether the connecting software is a human, an application or an AI agent. No client reaches protected data until source IP, user identity and session context are verified. A compromised or manipulated agent is no exception to this rule.

The caller does not matter

one rule, every client

| CLIENT                     | IDENTITY      | CONTEXT | RESULT |
|----------------------------|---------------|---------|--------|
| Human · SQL client         | ORDER_MANAGER | valid   | allow  |
| Application server         | ORDER_MANAGER | valid   | allow  |
| AI agent · copilot         | SVC_COPILOT   | missing | deny   |
| AI agent · prompt injected | ORDER_MANAGER | forged  | deny   |
| Scheduled job              | SVC_BATCH     | valid   | allow  |

The protection never asks what the caller is. It only checks whether all three conditions hold together.

Access denied

ERPAPP.EMP\_SALARY\_TAB

privileged account

User

DBA\_ADMIN

Privileges held

SELECT ANY TABLE, DBA

Paths attempted

direct SELECT → package → dynamic SQL

Session context

missing

DECISION: DENY

· privilege present, access refused — protection does not rely on grants

15:02:11

DBA\_ADMIN

SELECT

EMP\_SALARY\_TAB

deny

15:02:44

DBA\_ADMIN

EXEC

PKG\_HR\_UTIL.READ\_SALARY

deny

## Blocking administrator privilege

Privileged and shared users — DBAs included — are blocked from protected tables at the database level. AI integrations usually run under broadly privileged service accounts; with Data Castle those privileges are no longer a guarantee of access.

REGULATOR-READY REPORTING

Banking

Event summaries and sample ids mapped to supervision articles

Data protection

Personal-data articles, right-to-erasure and data-masking findings

PCI DSS v4

Audit-log requirements 10.2.1 / 10.2.2 / 10.2.4 / 10.2.7

Privileged access

DBA, SYS, SYSTEM and SYSDBA access with last-activity stamps

# For every installation holding sensitive data.

## *Runs without changing your architecture.*

Business units know the data is protected. Security, audit and IT teams get the determinability, separation of duties and audit trail they need to sign off.

### Value for every team

Without touching your existing architecture, from day one. **Example use cases:**

- **Information security**  
Privileged account risk closes at the database level; DBA privilege no longer means access to data.
- **Internal audit and compliance**  
Every access decision follows explicit, repeatable rules — defensible in front of financial regulators and supervisory authorities.
- **Database operations**  
Daily DBA work is unchanged; security policy moves to a separate identity and accountability becomes clear.
- **Application teams**  
Because protection works at object level, application code does not change and carries no extra integration risk.
- **AI and integration projects**  
Copilot and agent integrations cannot reach protected data even when they run under broadly privileged service accounts.
- **Finance and procurement**  
Requires no Database Vault, Audit Vault or Firewall licence.

### Trust and control

Your infrastructure. Your rules. Your data.

- **Three-layer protection**  
Network, table and non-removability layers work independently; all connections pass one gate and anomalous ones are cut in real time.
- **No model in the decision layer**  
100% rule-based, deterministic and repeatable. The outcome is predictable.
- **Bypass paths closed**  
The policy binds to the object; packages, procedures and dynamic SQL fall under the same control.
- **Separation of duties**  
The privilege to change a policy or grant an exemption is separate from the identity running the database.
- **Tamper-evident audit trail**  
Every access attempt and policy change is logged and bound to the previous event with blake3; chain integrity is verifiable.
- **On standard infrastructure**  
Built on the standard VPD capability of Enterprise Edition; requires no additional licence option.

**Free**  
Security  
assessment

Start with a 30-minute technical call. We scan the privileged access and bypass paths in your current installation together. At the end you receive a **findings report showing which tables are reachable through which paths.** No cost. No commitment.

**Book a 30-min slot →**

or reply to  
info@dbotech.uk