DATA SEC
ZERO TRUST SECURITY

Company Profile 2026

Build. Secure. Operate.

More than 150 organisations in the Kingdom rely on DataSec for their data centres, networks, IT operations and cybersecurity: one team that designs, builds, secures and operates, fluent in NCA, SAMA and PDPL requirements.

Managed SOC licensed by the National Cybersecurity Authority · Licence 010220341



Riyadh, Saudi Arabia datasec.sa

About DataSec

Infrastructure, security and operations, as one team

DataSec (legal name: AMN ALBAYANAT) is a Saudi infrastructure, networks and cybersecurity company headquartered in Riyadh. We design, build, secure and operate IT for government entities, banks, insurers and private enterprises across the Kingdom, and now offer secure AI services built to run under each client's own control.

Our mission

To turn technology and security from a list of products into measurable operational outcomes: systems that stay available, threats detected and contained, controls applied and evidenced, and decisions taken on clear data. We work from inside the Kingdom, with a team that understands its regulations and regulators, and we commit to every client through a written scope and defined responsibilities.

One partner from infrastructure to operations

1

One team from start to operations

No juggling several vendors: the same team assesses, designs, builds, secures and runs.

2

Deep knowledge of local regulation

We work to NCA controls, the SAMA framework and the Personal Data Protection Law.

3

We build on what you have

We integrate with your existing tools instead of imposing new platforms, and suggest additions only when justified.

4

Reports leadership understands

We turn technical detail into clear decisions and indicators you can track.

150+	450+	5+	27
organisations trust us	projects delivered	years of experience	specialist services

Frameworks and regulations we work to

NCA ECC · NCA CCC · SAMA CSF · PDPL · ISO 27001 · NIST CSF · CST CRF

Licence and trust

Licensed by the National Cybersecurity Authority

DataSec holds a Tier 2 licence to provide managed Security Operations Center services, one of a limited group of licensed providers in the Kingdom. The licence is listed in the NCA's official register.

Licence name

Managed Security Operations Center (MSOC) Services Licence — Tier 2

Licence no.	Valid
010220341	**14 July 2026 – 14 July 2031**

Verify on the NCA website

nca.gov.sa/en/registration-and-licensing

Look for "DataSec" under Tier 2.

Licence scope. A Tier 2 licence authorises the provision of managed SOC services to any organisation other than government entities and organisations that own, operate or host critical national infrastructure. We serve those organisations through advisory, assessment and solutions.

What the licence means for our clients

Around-the-clock operation from Riyadh

Our SOC operates from Riyadh around the clock, every day of the week and throughout the year, public holidays included.

Where monitoring data is kept

The licensing framework requires the service's monitoring data to stay inside the Kingdom. Your service agreement sets where your logs are kept (for example, on your own premises) and who may access them.

Connection to the national SOC

Our SOC is connected to the national cybersecurity operations centre, as the licensing framework requires.

Qualified Saudi analysts

The SOC is staffed by Saudi analysts qualified to the requirements of the National Cybersecurity Authority.

Log retention

We retain monitoring logs for the period the licensing framework sets, so they remain available for reference throughout that period.

Advance notice before any service discontinuation

The licensing framework obliges the provider to notify its clients in advance of any service discontinuation, within the periods and procedures the framework sets.

Other credentials

- **ISO 27001** — Information security
- **ISO 22301** — Business continuity
- **ISO 9001:2015** — Quality management
- **CST licence** — Communications, Space & Technology Commission
- **Local Content certificate**

How we work

From assessment to ongoing operations

Five stages show how our services connect. Start at the one you need, or let us help you identify where to begin.

27
services in 5 stages

Stage 1 · 3 services
Assess & Prioritise

What you need
Knowing where you stand before deciding what comes next.

What we do
We get to know your organisation, environment and applicable requirements, measure the gaps and set priorities.

What you gain
A clear picture of your current position, gaps and priorities.

Stage 2 · 4 services
Govern & Plan

What you need
Direction, ownership and rules that turn priorities into action.

What we do
We establish strategy, responsibilities, policies and risk management, and prepare your people to deliver the plan.

What you gain
An actionable plan, clear ownership and a framework for managing risk and compliance.

Stage 3 · 9 services
Build & Secure

What you need
A technical environment and security controls that match your plan.

What we do
We implement or improve your infrastructure and security controls, building on what you already have.

What you gain
The infrastructure and security solutions you need, implemented and integrated.

Stage 4 · 3 services
Test & Validate

What you need
Evidence that your controls work as intended.

What we do
We test how well your controls hold up, find remaining weaknesses and verify the fixes.

What you gain
Evidence of how your defences perform and clear findings to address.

Stage 5 · 8 services
Operate & Improve

What you need
Reliable day-to-day operations, with threats watched and handled.

What we do
We run and support your IT, monitor and respond to threats, manage vulnerabilities and keep improving.

What you gain
Ongoing operations, monitoring, response and measurable improvement.

Secure AI follows the same path: readiness and governance first, platforms built and tested before go-live, then run and measured.

The stages are a guide, not prerequisites: choose only the services you need.

Facing an active incident? Start with Incident Response · datasec.sa/en/services/incident-response →

Services

Six pillars, one team

Every service has its own page on datasec.sa with its scope, deliverables and answers to common questions.

27
services in 6 pillars

01 — 4 services

Assess & Test

Find the gaps before someone else does, with a clear scope and an actionable report.

- Penetration Testing →
- Red Team →
- Cloud Security Assessment →
- Vulnerability Management →

02 — 4 services

Govern & Comply

From NCA controls to SAMA and PDPL: compliance built to last.

- GRC Advisory →
- Compliance Assessment →
- Third-Party Risk & GRC Platform →
- Awareness & Training →

03 — 4 services

Security Solutions

Design and delivery of network security, data protection, and identity and access solutions.

- Network Security & Micro-Segmentation →
- Data Security →
- Generative AI Data Protection →
- Identity & Access →

04 New — 8 services

Secure AI & Automation

We design, build, secure and operate private AI platforms, governed access to models, enterprise knowledge systems and controlled automation for regulated organisations.

- AI Strategy & Readiness Assessment →
- AI Governance & Regulatory Readiness →
- Private & Sovereign AI Platforms →
- Secure AI Gateway & Guardrails →
- Enterprise Knowledge AI & Document Intelligence →
- AI Agents & Workflow Automation →
- AI Security Assessment & Red Teaming →
- Managed AI Platforms & LLMOps →

05 — 3 services

IT Infrastructure & Managed Operations

We build, run and monitor your technology estate to security standards: from data centres and networks to ongoing support and a network operations centre.

- Infrastructure →
- Managed IT Services →
- Network Operations Center (NOC) →

The NOC watches the availability and performance of networks and systems; security monitoring belongs to Detect & Respond.

06 — 4 services

Detect & Respond

Continuous monitoring, analysis and response from our SOC in Riyadh.

- Managed SOC →
- Managed Detection & Response (MDR) →
- Incident Response →
- Threat Intelligence & Brand Protection →

Managed SOC and MDR are delivered under our Managed Security Operations Center (MSOC) Services Licence — Tier 2, which excludes government entities and organisations that own, operate or host critical national infrastructure.

Secure AI & Automation

Secure AI: assess, govern and build

AI that stays under your control: we help you choose the use cases worth building, govern them and build them on your own infrastructure.

8
Secure AI services

Assess & Prioritise

AI Strategy & Readiness Assessment →

Find the AI use cases worth building: readiness and data assessment, prioritised use cases, a target architecture and a roadmap with budget considerations.

Govern & Plan

AI Governance & Regulatory Readiness →

AI policies, a system inventory, risk classification, human oversight and evidence mapped to the Saudi requirements that apply to you.

Build & Secure

Private & Sovereign AI Platforms →

AI platforms on infrastructure you control: locally deployed models, isolation and integration, with every external dependency documented.

Build & Secure

Secure AI Gateway & Guardrails →

One governed path to approved models: identity-based access, prompt and output policies, sensitive-data redaction, audit logs, and usage and cost limits.

Build & Secure

Enterprise Knowledge AI & Document Intelligence →

Arabic and English assistants that answer from your own documents with their sources and existing permissions, plus document extraction.

Where the AI runs

Four deployment options, each with one fixed definition that we use in every proposal and design.

1. **Private hosting**
   A dedicated environment for you alone, on your premises or with a host you choose. Any outside service it still calls is listed.
2. **Saudi data residency**
   Data stored and processed in the Kingdom. Every service outside it, and the data that service receives, is named.
3. **Sovereign**
   Residency, with encryption keys, administration and change control held by you or a party you approve in the Kingdom.
4. **Air-gapped**
   No network path to outside services. Models run locally, and updates arrive on controlled media after they are checked.

We state which option a design meets and what remains outside it. Whether it satisfies a regulation is for your organisation and its regulator to conclude, with the evidence we provide.

Secure AI & Automation

Secure AI: automate, test and operate

Agents that act only within the limits you set, independent testing before go-live, and operations that measure the platform and report its usage and cost against your budget.

8
Secure AI services

Build & Secure

AI Agents & Workflow Automation →

Agents that act in your systems only within set limits: least-privilege access, human approval for sensitive actions and a full audit trail.

Test & Validate

AI Security Assessment & Red Teaming →

Authorised testing of assistants, agents and AI applications for prompt injection, data exposure, cross-user access and tool misuse, with retesting.

Operate & Improve

Managed AI Platforms & LLMOps →

Running AI platforms after go-live: monitoring, evaluation on every change, controlled updates, backup and recovery, and capacity and cost reporting.

How an engagement grows

01
Discovery
A readiness and data assessment, use cases ranked by value, effort and risk, a target architecture, and acceptance criteria for a proof of concept.

02
Proof of concept
A limited scope on your data, measured against acceptance criteria agreed in advance: answer quality and grounding, access isolation, unsafe-action prevention, performance and cost.

03
Production
A build on the chosen deployment option, security testing before go-live, and handover with runbooks and documentation.

04
Managed operation
If you need it: monitoring, evaluation, controlled updates, backup and recovery, with scope, responsibilities and support hours set in the contract.

Written down before anything is built

For each kind of data: where it lives, who can read it and how long it is kept.

- **Prompts and answers** — Where processed, whether stored, and training terms
- **Documents** — Source systems, copies made, who can retrieve them
- **Embeddings and indexes** — Where the index sits; protected like its source
- **Logs and audit records** — What is logged, for how long, who reads it
- **Backups** — Location, encryption, key holders, restore test
- **Telemetry and support access** — What leaves the environment, and why

Staff using public AI tools? **Generative AI Data Protection**, in Security Solutions, blocks or warns when sensitive data is sent to them.

The eight Secure AI services in detail · datasec.sa/en/ai →

Our clients

Organisations we have served

A selection of the 150+ government entities, banks, insurers and leading enterprises in Saudi Arabia that DataSec has served in cybersecurity and IT.

450+ projects delivered

5+ years of experience

27 specialist services

Government

Banking

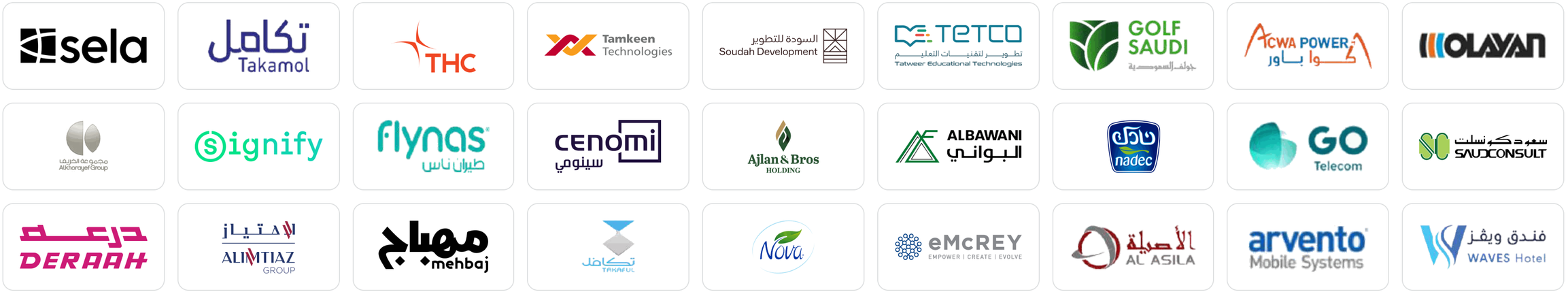
The logos shown are a selection of our clients, not a complete list. They show a working relationship with DataSec across our different services; they do not mean every organisation uses every service.

More of our clients

Insurance and Finance



Enterprise



The logos shown are a selection of our clients, not a complete list. They show a working relationship with DataSec across our different services; they do not mean every organisation uses every service.

Technology

Our technology partners

We design, deliver and support solutions from these companies. A selection, not a complete list.

Network security

FORTINET · paloalto NETWORKS · Akamai · FORESCOUT · CLOUDFLARE · f5 · imperva · Barracuda · proofpoint · MENLO SECURITY · VECTRA · EXTRAHOP · wallarm · Infoblox

Endpoint & data security

CROWDSTRIKE · SentinelOne · TREND MICRO · kaspersky · ZIMPERIUM · BROADCOM · THALES · Forcepoint · IBM · SECLORE · FORTRA · SEARCHINFORM RISK AND COMPLIANCE MANAGEMENT · GTB Technologies Next Gen Data Protection

Identity & access

Saviynt · SailPoint · BeyondTrust · Delinea · RSA · Arcon · CEREBRA سيريبرا

Threat intelligence

Recorded Future · GROUP-IB · BRANDEFENSE · SCANWAVE · ZINAD Protection is our profession · Defensys · JETHUR جذور

Infrastructure

cisco · NUTANIX · HPE aruba networking · citrix · veeam

SIEM & log management

splunk> · LogRhythm · seceon · Cribl

Vulnerability, GRC & awareness

tenable · GRC Orbit · dPhish

IT management

opentext™ · ivanti · ZOHO · riverbed · AXONIUS

DATA SEC
ZERO TRUST SECURITY

Let’s talk about what you need

Send us your enquiry through the form on datasec.sa, on WhatsApp, by phone or by email.

Three steps from request to plan

1

Request a consultation

Tell us what you need through the form, WhatsApp, phone or email.

2

Assessment session

We understand your environment and regulatory requirements and define the scope with you.

3

Plan and proposal

You receive a clear plan with scope, deliverables and timeline.

Contact DataSec

Unified number (within Saudi Arabia)
9200 33782

Mobile (calls and WhatsApp)
+966 59 750 4669

Email
info@datasec.sa

Website
datasec.sa

LinkedIn
linkedin.com/company/datasecc

Address
3173 Al Abbas Ibn Abdulmutalib, At Taawun, Riyadh 12475, Saudi Arabia

AMN ALBAYANAT · CR 1010752666 · Unified establishment number 7026307020

How we work with you

Clarity

A written scope, defined responsibilities and reports that say what happened and what did not.

Outcomes, not products

We do not sell licences and leave. We commit to an operational result: asset coverage, vulnerability remediation and review-ready compliance evidence.

Continuity

Security is a process, not a project, so we measure improvement over time and review priorities with you regularly.

A team in the Kingdom

Our team works from Riyadh, speaks the language of Saudi regulators and their requirements, and works with you in Arabic or English as you prefer.

EXA GROUP
Build.Trust.Execute

DataSec is part of EXA Group, alongside ExaHost, ExaCall and Bayanat.

EXA host · exa call · Bayanat