EmaLite

SERVICE BROCHURE

Cyber security

Security architecture built into the design rather than bolted on afterwards — segmentation, inspection and identity, arranged around where your data actually lives.

What we are usually called in for

Most breaches exploit architecture, not zero-days. An attacker who reaches one machine on a flat network has reached all of them; the sophistication was never required. Meanwhile the firewall rule base has been growing for a decade, nobody will remove a rule because nobody knows what it is for, and the answer to "what can this server reach" takes an afternoon to work out.

Adding another product rarely fixes this. The control that matters is the boundary, and boundaries are a design decision.

Our approach

We begin with where the data sits and who genuinely needs it — not with a product list. From there the work is structural: zones with a real boundary between them, inspection at the points that count, and access decided by identity rather than by which port someone plugged into.

Then we prove it. A control nobody has tested is a control nobody should be relying on, and a rule base nobody can explain is an audit finding waiting for its turn.

What the work involves

Perimeter & next-generation firewalls

Policy design, rule-base rationalisation and inspection strategies that survive change management rather than being worked around by it.

Segmentation & zero-trust access

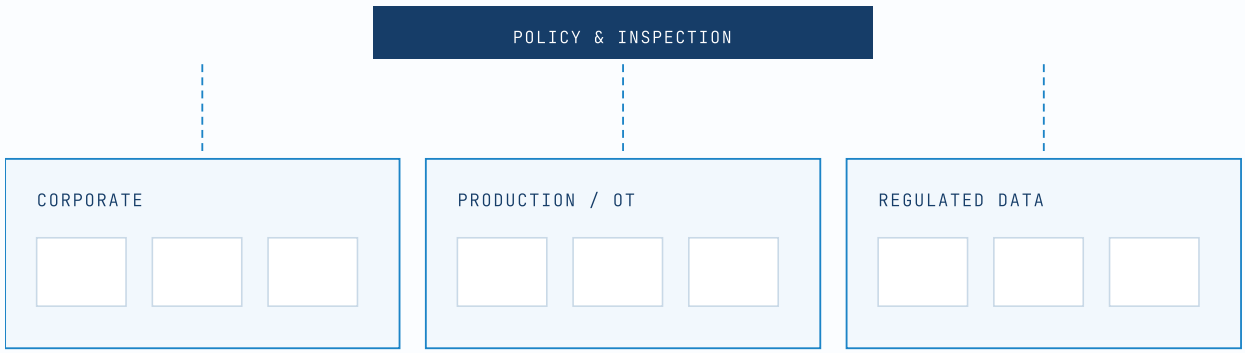
East-west control between zones, identity-aware access for users and machines, remote access that is not simply a flat VPN with a password.

Detection & response

IDS/IPS, endpoint protection and log pipelines feeding a monitored workflow with defined escalation and owners who are named.

Assessment & assurance

Architecture review, vulnerability assessment and configuration audit, mapped to the frameworks you actually report against.



SEGMENTATION — TRAFFIC BETWEEN ZONES IS MATCHED AGAINST POLICY RATHER THAN TRUSTED BY DEFAULT

How it is sequenced

STAGE	WHAT HAPPENS
Assess	Where data sits, who reaches it today, and what the current rule base actually permits
Design	Zones, boundaries, inspection points and access model — documented before anything changes
Rationalise	Rules mapped to documented flows; what cannot be explained is retired, not carried forward
Enforce	Policy applied in controlled stages, with a way back at each one
Prove	Controls tested, access paths verified, evidence written up for whoever asks next

What is delivered

Every engagement ends with something you keep. For this service, that is:

- A named, testable boundary — the blast radius stated rather than assumed
- A rationalised rule base you can explain, rule by rule, to an auditor
- Access paths documented, including the ones that surprised everyone
- Alerting tuned to signal rather than volume, with escalation that has owners
- Evidence: test results, not a policy document asserting that controls exist

Technologies

NGFW | CISCO SECURITY | ZERO TRUST | IDS / IPS | EDR | SIEM | MICRO-SEGMENTATION | TLS INSPECTION

> ON COMPLIANCE
>
> Regulatory alignment is an outcome of a well-documented architecture, not a separate workstream bolted on before an audit. If the design is right and written down, most of the evidence already exists.

EmaLite

Start with the estate you actually have.

EMAIL

hello@emalite.com

TELEPHONE

+966 11 000 0000

OFFICE

Al Olaya, Riyadh, Kingdom of Saudi Arabia

WEB

emalite.com

Send us the current topology, or the problem you cannot get past, and we will tell you what we would do about it.