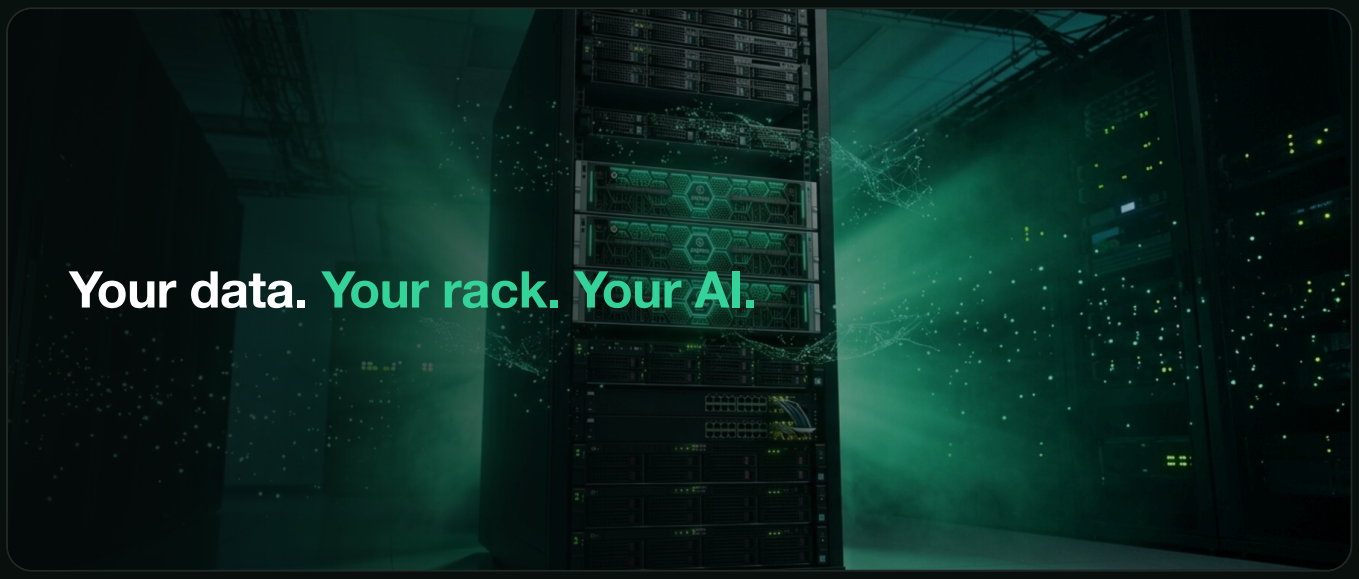
SOVEREIGN AI RACK SERVERS

Powerful AI. Inside your building. Nothing leaves.

Sigmix Sovereign Appliance — a single, sealed on-premises server running a full generative-AI suite inside your data centre, with **zero internet egress**. Built for any organisation that wants the latest AI while keeping **100% control** of its data and infrastructure — inside its own walls.

- Zero internet egress
- Processed in-Kingdom
- Bilingual · AR / EN
- Turnkey · weeks not years



FOUR TIERS, SIZED TO YOUR ORGANISATION

TIER	FOOTPRINT	AI ACCELERATORS	INDICATIVE USERS*	BEST FOR
S	2U	1	~200–250	A department or team
M	2U	2–3	~500–750	A division / mid-size org
L	4U	4–6	~1,500–2,500	Enterprise-wide
XL	4U	8	~2,500–3,500+	High concurrency

*Indicative at ~10% peak concurrency; final sizing validated to your usage. All tiers include all 7 modules, full EN/AR bilingual, and zero-egress + audit + SIEM.

THE SUITE — RUNNING ON YOUR METAL

AI Chat
A private assistant your teams can use with sensitive information.

Documents & Knowledge (RAG)
Ask across your own documents, with permissions that respect who sees what.

Image & Social Creator
On-brand images and ready-to-post content, in Arabic and English.

Video & Advert Creator
Short videos and adverts, generated entirely on your own hardware.

Document Creator
Structured, polished documents and reports from a simple prompt.

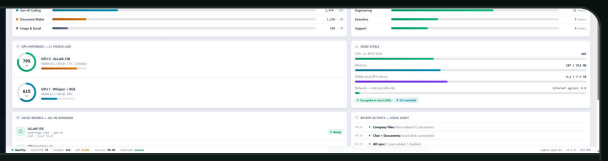
Fully bilingual
The whole experience — native Arabic & English, full right-to-left.

INSIDE THE CONSOLE — THE SEALED CONTROL PLANE

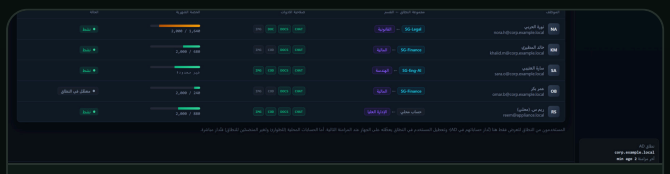
One bilingual admin console; every request served on-box, a persistent NO EGRESS · AIR-GAPPED status, in English or Arabic, light or dark.

Overview · Performance & Health — live service metrics, every request served on-box.

- Live KPIs — active users, throughput, p95/p99 latency, success rate, queue



- Node vitals — GPU utilisation, VRAM & temperature, internet egress 0 B, LUKS

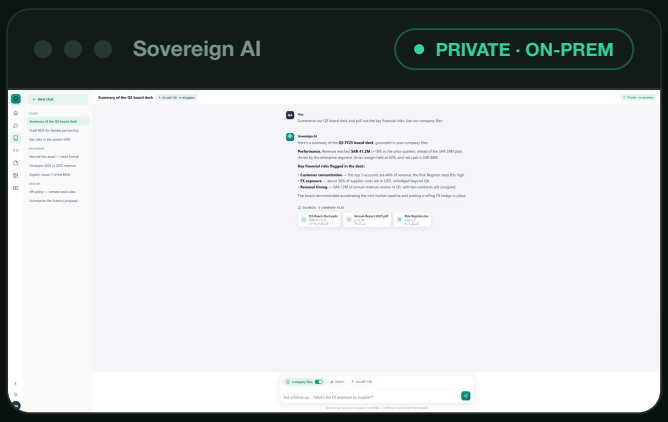


- Employees & Access — Active Directory (LDAPS), per-tool access, quotas

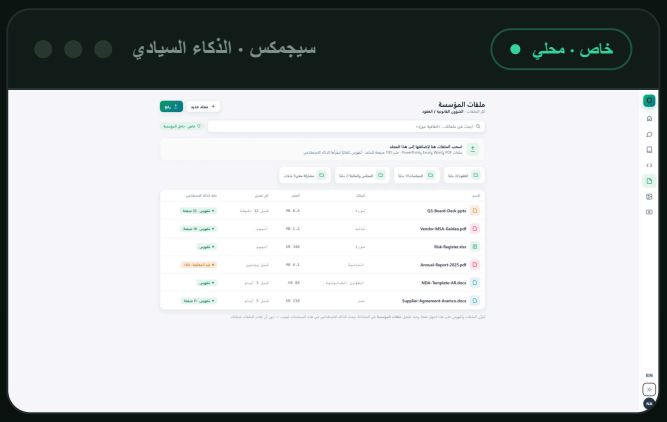
- System — Ed25519 license (no phone-home) + atomic A/B firmware, ZFS/LUKS storage

THE EXPERIENCE — PRIVATE, GROUNDED, NATIVELY BILINGUAL

AI Chat answers only from your own files; the entire app works natively in Arabic and English with full right-to-left support.



AI Chat (English) — grounded in company files, with sources



Documents & Knowledge (RAG) — native Arabic, full RTL

DEPLOY ON-PREMISES, OR IN YOUR COLOCATION FACILITY

On-premises server room

Sovereign colocation cage

Racked in your data centre

GPU cluster at scale

TECHNICAL SPECIFICATIONS

Network · Zero Trust

- Default-deny egress firewall; no outbound internet in sealed mode
- Continuous egress canary; LAN-only exposure; internal-CA / mTLS
- DNS restricted to approved resolvers; VLAN / air-gap deployable

Cryptography

- FIPS 140-3 validated modules (NIST CMVP certificate reference)
- LUKS full-disk, TPM-sealed; TLS 1.2+/1.3, FIPS ciphers; SME/SEV where validated
- Customer-sole custody of the recovery key; NCA-crypto configurable

Platform hardening

- RHEL minimal install, CIS Benchmark / DISA STIG; SELinux enforcing
- Secure Boot + Silicon Root of Trust + signed firmware; System Lockdown
- Secured Component Verification; chassis intrusion + bezel lock

Identity & access

- AD (LDAPS) offline; local + offline signed user-import; hybrid-Entra
- RBAC + row-level isolation; RAG ACLs enforced pre-retrieval & pre-prompt
- Admin MFA/TOTP; scoped, capped API keys; break-glass (no fixed backdoor)

Supply-chain integrity

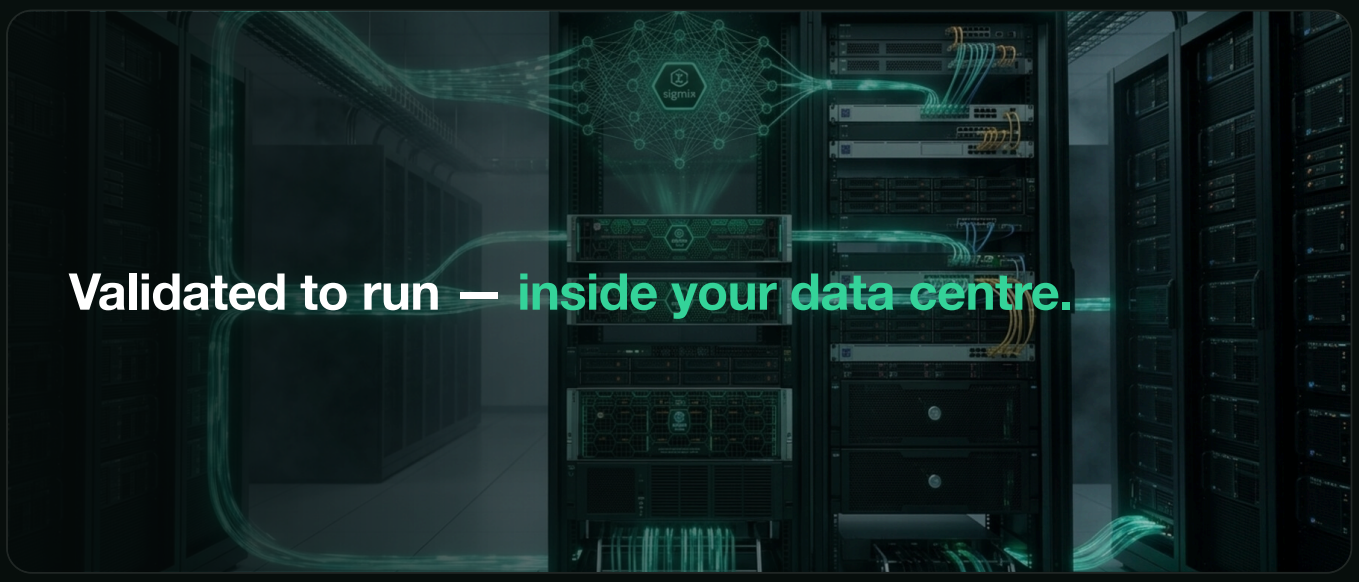
- Signed, transactional A/B updates with automatic rollback
- Split signing-key hierarchy (offline root + HSM-held keys)
- SHA-256-verified model weights; SBOM + CVE/VEX; signed provenance (SLSA/in-toto)

Logging, detection & recovery

- Hash-chained, tamper-evident audit; daily WORM / SIEM anchor; syslog/CEF or OCSF
- GPU/host telemetry (DCGM); fault quarantine + PII-redacted support bundles
- Redundant PSUs, ECC, RAID-1, PLP NVMe; deterministic power-loss recovery

LOCAL MODELS — ALL IN-KINGDOM

Ships with **ALLaM** (sovereign Arabic chat) · **Whisper large-v3** (speech) · **BGE-M3** (embeddings / RAG) · **FLUX** (image). Swap-in offline: Qwen2.5, Llama-3.3 — all signed & SHA-256-verified before load.



SIGMIX GUARD™ — OUR OWN HARDWARE, OUR OWN FIRMWARE

Beyond the validated server, an **independent layer** scrubs sensitive data and anchors a tamper-evident audit trail on every Sigmix appliance today — and our own proprietary **PCIe card**, running Sigmix-authored firmware, brings that layer into **dedicated hardware**, separate from the host operating system. Purpose-built, brandable, and sovereign by design.

- Sigmix-authored firmware
- Non-Chinese sourced
- Independent of the host OS

TWO JOBS — IN DEDICATED HARDWARE, OR IN SOFTWARE

Independent PII & data scrubbing

National ID / Iqama, IBAN, payment-card and credential patterns are detected and redacted before documents enter your knowledge base or a response leaves the box — designed to support your PDPL, NCA & SAMA obligations.

Tamper-evident audit anchoring

Every request is hashed into a chained audit anchor; the appliance's FIPS-validated TPM 2.0 signs the exported anchor, which replicates to your SIEM / WORM store — an independent integrity record.

Never a single point of failure

If the card is ever absent or faulted, the identical protection runs in software on the same box. Inference is never blocked; the safeguard is never lost.

A full-height PCIe card — designed to install in any Sigmix appliance

An independent enforcement & integrity layer, on-box

Sovereign, by design. A Sigmix-branded PCIe FPGA card — custom bracket, silkscreen and PCIe vendor ID, so it identifies as Sigmix inside your rack; sourced from a non-Chinese vendor, with an AES-256 + eFUSE-protected firmware bitstream. It is an independent enforcement layer — **not** the certified root of trust, which remains the appliance's FIPS-validated TPM. **Availability:** the scrubbing & audit-anchor layer ships with every appliance today in software; the hardware-accelerated card is a parallel track that adds acceleration and the Sigmix brand as it lands — it never gates a deployment.

SECURITY — SEALED BY DESIGN, ZERO TRUST-ALIGNED

- ✓ **Zero internet egress**
  Default-deny; a continuous canary alerts only if the internet becomes reachable.
- ✓ **Hardware root of trust**
  Silicon RoT → Secure Boot → measured boot → TPM-sealed disk.
- ✓ **FIPS-validated cryptography**
  NIST CMVP-listed modules, FIPS mode enforced.
- ✓ **Encrypted everywhere**
  LUKS at rest, TLS 1.3 & mTLS in transit.
- ✓ **Least-privilege**
  RBAC + row-level isolation, RAG ACLs enforced twice, admin MFA.
- ✓ **No vendor backdoor**
  No remote access, no vendor-held key, no phone-home.

COMPLIANCE — BUILT TO SUPPORT THE KINGDOM'S REGULATORS

Designed to help you meet: SAMA CSF · NCA ECC-2:2024 · PDPL · NDMO data-localization

Aligned with the principles of: ISO/IEC 27001 · ISO/IEC 42001 (AI) · NIST CSF · Vision 2030 objectives

Per-deployment evidence pack:

- SAMA CSF mapping
- NCA ECC-2 mapping
- PDPL / ROPA
- CIS / STIG scan
- FIPS certificate ref
- SBOM
- CVE / VEX
- Secure Boot / TPM status
- Zero-egress test
- SIEM export sample
- Access-review sample
- Model-license register

Honest by design. We don't claim to be "SAMA-approved," "NCA-certified" or a "FIPS-certified appliance" — these frameworks assess your organisation, and FIPS validation covers the cryptographic modules, not the whole box. The ISO/NIST references above are statements of alignment with those standards' principles, not certifications we hold. This is a single-node appliance with component redundancy (not a high-availability cluster); for continuous availability, run two independent units behind your load balancer.

ENTERPRISE FOUNDATIONS — VALIDATED BEFORE IT SHIPS

Built on **NVIDIA-qualified Dell PowerEdge** hardware and a hardened **Red Hat Enterprise Linux** foundation — hardware root of trust, Secure Boot, TPM 2.0, CIS/STIG-hardened, put through a defined validation gauntlet (thermal at Kingdom ambient, 100× unattended reboot, power-cut recovery, zero-egress verification, measured sizing).

CLOUD AI VS. THE SIGMIX SOVEREIGN APPLIANCE

	CLOUD AI	SIGMIX SOVEREIGN APPLIANCE
Where data goes	To the provider's cloud	**Never leaves your rack**
Internet dependency	Required	**None (sealed)**
Vendor access to data	Yes	**None**
Audit / SIEM	Provider-controlled	**Your logs, your SIEM**
Identity	Provider accounts	**Your Active Directory**

SIGMIX — KINGDOM OF SAUDI ARABIA

7229 — King Abdullah Financial District
Innovation Boulevard · 3004 — Al Aqeeq District
13519 — Riyadh, Kingdom of Saudi Arabia

CR / UNIFIED NO.
7054521799

VAT ID
314836510700003

WEBSITE
sigmix.sa

EMAIL
contact@sigmix.sa

TELEPHONE
+966 11 525 6806

Book a technical briefing →

خوادم الذكاء الاصطناعي السيادية

ذكاء اصطناعي قوي.
داخل مبناك.
لا شيء يغادر.

جهاز سيجمكس السيادي — خادم واحد مُحكم يُشغّل مجموعة كاملة من أدوات الذكاء الاصطناعي التوليدي داخل مركز بياناتك، مع **صفر خروج للإنترنت**. مُصمّم لأي مؤسسة تريد أحدث تقنيات الذكاء الاصطناعي مع الاحتفاظ بـ**السيطرة الكاملة (100%)** على بياناتها وبنيتها التحتية — داخل جدرانها.

- صفر خروج للإنترنت
- معالجة داخل المملكة
- ثنائي اللغة · عربي / إنجليزي
- جاهز للتشغيل · أسابيع لا سنوات

أربع فئات بمقاسات تناسب مؤسستك

الفئة	المساحة	مسرّعات الذكاء	المستخدمون (تقديري)*	الأنسب لـ
S	2U	1	~200–250	قسم أو فريق
M	2U	2–3	~500–750	إدارة / مؤسسة متوسطة
L	4U	4–6	~1,500–2,500	على مستوى المؤسسة
XL	4U	8	~2,500–3,500+	تزامن عالٍ

*تقديري عند ذروة تزامن ~10٪؛ يُحدَّد الحجم النهائي وفق استخدامك. تشمل جميع الفئات الوحدات السبع، وثنائية اللغة الكاملة، وصفر الخروج + التدقيق + SIEM.

المجموعة — تعمل على أجهزتك

محادثة ذكية
مساعد خاص يمكن لفرقك استخدامه مع المعلومات الحساسة.

المستندات والمعرفة (RAG)
اسأل عبر مستنداتك الخاصة، بصلاحيات تحترم من يرى ماذا.

منشئ الصور والمحتوى الاجتماعي
صور احترافية ومحتوى جاهز للنشر، بالعربية والإنجليزية.

منشئ الفيديو والإعلانات
مقاطع فيديو وإعلانات قصيرة، تُنشأ بالكامل على أجهزتك.

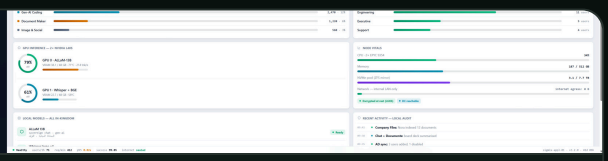
منشئ المستندات
مستندات وتقارير منظّمة ومصقولة من وصف بسيط.

ثنائي اللغة بالكامل
التجربة كاملة — عربية وإنجليزية أصيلة، دعم كامل لليمين لليسار.

داخل لوحة التحكم — لوحة التحكم المُحكمة

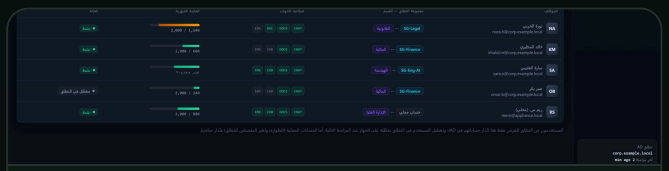
لوحة تحكم واحدة ثنائية اللغة؛ كل طلب يُخدَم على الجهاز، مع شارة صفر خروج · معزول دائمة، بالعربية أو الإنجليزية، فاتحة أو داكنة.

نظرة عامة · الأداء والصحة — مؤشرات حية، كل طلب يُخدَم على الجهاز.



- مؤشرات حية — المستخدمون، الإنتاجية، زمن p95/p99، معدل النجاح، الطابور

- حيوية العقدة — استخدام المعالج، الذاكرة والحرارة، خروج إنترنت 0 بايت، LUKS

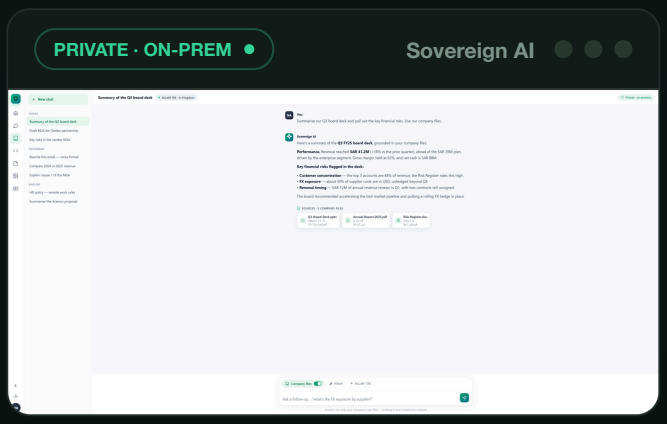


- الموظفون والوصول — Active Directory (LDAPS)، وصول لكل أداة، حصص

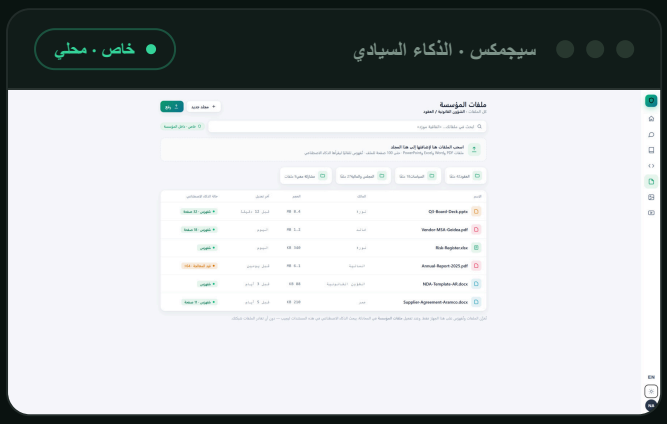
- النظام — ترخيص Ed25519 (بلا اتصال تلقائي) + برنامج ثابت A/B، تخزين ZFS/LUKS

التجربة — خاصة، مبنية على ملفاتك، ثنائية اللغة

المحادثة الذكية تجيب من ملفاتك فقط؛ التطبيق بالكامل يعمل بالعربية والإنجليزية مع دعم كامل لليمين لليسار.



المحادثة الذكية (إنجليزي) — مبنية على ملفات الشركة، مع المصادر



المستندات والمعرفة (RAG) — عربي أصيل، RTL كامل

النشر داخلياً أو في منشأة استضافة سيادية

غرفة خوادم داخلية

قفص استضافة سيادي

في خزانة مركز بياناتك

عنقود معالجات بمقياس كبير

المواصفات التقنية

الشبكة · الثقة الصفرية

- جدار منع خروج افتراضي؛ لا اتصال إنترنت صادر في الوضع المُحكم
- مراقب خروج مستمر؛ كشف على الشبكة المحلية فقط؛ CA داخلية / mTLS
- DNS مقيّد بمحلّلات معتمدة؛ قابل للنشر مع VLAN / عزل تام

تقوية المنصّة

- RHEL بتثبيت أدنى، CIS / DISA STIG؛ SELinux في وضع الفرض
- إقلاع آمن + جذر ثقة سيليكوني + برامج ثابتة موقّعة؛ قفل النظام
- التحقق من سلامة المكوّنات؛ كشف عبث الهيكل + قفل الواجهة

سلامة سلسلة التوريد

- تحديثات A/B موقّعة مع تراجع تلقائي
- هرمية مفاتيح توقيع مقسّمة (جذر دون اتصال + مفاتيح في HSM)
- أوزان مُتحقَّقة بـ SHA-256؛ SBOM + CVE/VEX؛ إثبات منشأ (SLSA/in-toto)

التشفير

- وحدات معتمدة FIPS 140-3 (مرجع شهادة NIST CMVP)
- LUKS كامل القرص، مختوم بـ TPM؛ TLS 1.2+/1.3؛ SME/SEV حيث يُعتمد
- حيازة العميل الحصرية لمفتاح الاسترداد؛ قابل للضبط وفق معايير NCA

الهوية والوصول

- AD (LDAPS) دون اتصال؛ استيراد مستخدمين موقّع؛ Entra هجين
- تحكم بالأدوار + عزل على مستوى الصف؛ صلاحيات RAG قبل الاسترجاع والتلقين
- مصادقة ثنائية للمشرف؛ مفاتيح API مُقيّدة؛ زجاج الكسر (دون باب خلفي)

التسجيل والكشف والتعافي

- تدقيق متسلسل بالتجزئة؛ مرساة WORM / SIEM يومية؛ syslog/CEF أو OCSF
- قياس عن بُعد (DCGM)؛ عزل الأعطال + حزم دعم مُنقّاة من PII
- مزوّدات مكرّرة، NVMe ،RAID-1، ECC محمي؛ تعافٍ حتمي من فقد الطاقة

النماذج المحلية — كلها داخل المملكة

يأتي مع **ALLaM** (محادثة عربية سيادية) · **Whisper large-v3** (تفريغ صوتي) · **BGE-M3** (تضمين / RAG) · **FLUX** (صور). تبديل دون اتصال: Qwen2.5، Llama-3.3 — جميعها موقّعة ومُتحقَّقة بـ SHA-256 قبل التحميل.

سيجمكس جارد™ — عتادنا الخاص، وبرنامجنا الثابت

إلى جانب الخادم المُتحقَّق منه، تقوم **طبقة مستقلة** بتنقية البيانات الحساسة وترسيخ سجل تدقيق مقاوم للعبث في كل جهاز سيجمكس اليوم — كما تنقل بطاقتنا الخاصة **PCIe**، التي تعمل ببرنامج ثابت من تأليف سيجمكس، هذه الطبقة إلى **عتاد مخصّص** منفصل عن نظام التشغيل المضيف. مبنية لغرضها، قابلة للعلامة التجارية، وسيادية بالتصميم.

- برنامج ثابت من سيجمكس
- مصدر غير صيني
- مستقلة عن نظام التشغيل

مهمّتان — في عتاد مخصّص أو في البرمجيات

تنقية مستقلة للبيانات الحساسة

تُكتشف وتُحجب أنماط الهوية الوطنية / الإقامة والآيبان وبطاقات الدفع وبيانات الاعتماد قبل دخول المستندات إلى قاعدة معرفتك أو مغادرة أي رد للجهاز — مصمّمة لدعم التزاماتك وفق PDPL وNCA وSAMA.

ترسيخ تدقيق مقاوم للعبث

يُجزّأ كل طلب في مرساة تدقيق متسلسلة؛ ويوقّع الـ TPM 2.0 المعتمد وفق FIPS في الجهاز المرساةَ المُصدَّرة، التي تتكرّر إلى SIEM / مخزن WORM — سجل سلامة مستقل.

ليست نقطة فشل واحدة أبداً

إذا غابت البطاقة أو تعطّلت، تعمل الحماية نفسها برمجياً على الجهاز ذاته؛ لا يُحجب الاستدلال أبداً، ولا تُفقد الحماية.

بطاقة PCIe كاملة الارتفاع — مصمّمة للتركيب في أي جهاز سيجمكس

طبقة إنفاذ وسلامة مستقلة، على الجهاز

سيادية بالتصميم. بطاقة FPGA بعلامة سيجمكس — حامل مخصّص وطباعة سطحية ومعرّف مورّد PCIe، لتُعرّف بأنها سيجمكس داخل خزانتك؛ من مصدر غير صيني، ببرنامج ثابت محمي بـ AES-256 وeFUSE. إنها طبقة إنفاذ مستقلة — **وليست** جذر الثقة المعتمد، الذي يبقى الـ TPM المعتمد وفق FIPS في الجهاز. **التوافر:** تُشحن طبقة التنقية والتدقيق مع كل جهاز اليوم برمجياً؛ والبطاقة المُسرَّعة عتادياً مسار موازٍ يضيف التسريع وعلامة سيجمكس عند توفّرها — ولا تعطّل أي عملية نشر أبداً.

الأمن — مُحكم بالتصميم، متوافق مع مبدأ الثقة الصفرية

- ✓ **صفر خروج للإنترنت**
  منع افتراضي؛ مراقب ينبّه فقط إذا أصبح الإنترنت قابلاً للوصول.
- ✓ **جذر ثقة عتادي**
  جذر سيليكوني ← إقلاع آمن ← إقلاع مُقاس ← قرص مختوم بـ TPM.
- ✓ **تشفير معتمد وفق FIPS**
  وحدات مُدرجة في NIST CMVP، مع تفعيل وضع FIPS.
- ✓ **تشفير في كل مكان**
  LUKS للتخزين، TLS 1.3 وmTLS أثناء النقل.
- ✓ **أقل الصلاحيات**
  تحكم بالأدوار + عزل على مستوى الصف، صلاحيات RAG مرتين، مصادقة ثنائية.
- ✓ **بدون باب خلفي**
  لا وصول عن بُعد، لا مفتاح لدى المورّد، لا اتصال تلقائي.

الامتثال — مبني لدعم الجهات التنظيمية في المملكة

مُصمّم لمساعدتك على تلبية:

- **إطار SAMA للأمن السيبراني**
- **ضوابط NCA ECC-2:2024**
- **نظام حماية البيانات PDPL**
- **توطين البيانات NDMO**

متوافق مع مبادئ:

- **ISO/IEC 27001**
- **ISO/IEC 42001 (الذكاء)**
- **إطار NIST**
- **مستهدفات رؤية 2030**

حزمة الأدلة لكل عملية نشر:

- مطابقة SAMA CSF
- مطابقة NCA ECC-2
- PDPL / ROPA
- فحص CIS / STIG
- مرجع شهادة FIPS
- SBOM
- CVE / VEX
- حالة الإقلاع الآمن / TPM
- اختبار صفر الخروج
- عينة تصدير SIEM
- عينة مراجعة الوصول
- سجل تراخيص النماذج

صادقون بالتصميم. لا ندّعي أننا «معتمدون من البنك المركزي» أو «معتمدون من الهيئة الوطنية للأمن السيبراني» أو «جهاز معتمد وفق FIPS» — فهذه الأطر تُقيّم مؤسستك، واعتماد FIPS يغطي الوحدات التشفيرية لا الجهاز بأكمله. والإشارات إلى ISO/NIST أعلاه بيانات توافق مع مبادئ تلك المعايير، وليست شهادات نمتلكها. هذا جهاز أحادي العقدة مع تكرار للمكوّنات (وليس عنقوداً عالي التوافر)؛ ولاستمرارية التوافر، شغّل وحدتين مستقلتين خلف موازن الأحمال.

أسس مؤسسية — مُتحقَّق منها قبل الشحن

مبني على عتاد **Dell PowerEdge** المعتمد من **NVIDIA** وأساس **Red Hat Enterprise Linux** المُقوّى — جذر ثقة عتادي، إقلاع آمن، TPM 2.0، تقوية CIS/STIG، ويمرّ عبر مسار تحقق مُحدَّد (اختبار حراري عند درجات حرارة المملكة، 100 إعادة تشغيل دون إشراف، تعافٍ من انقطاع الكهرباء، التحقق من صفر الخروج، قياس الحجم فعلياً).

الذكاء السحابي مقابل جهاز سيجمكس السيادي

	الذكاء السحابي	جهاز سيجمكس السيادي
أين تذهب البيانات	إلى سحابة المزوّد	**لا تغادر خادمك أبداً**
الاعتماد على الإنترنت	مطلوب	**لا شيء (مُحكم)**
وصول المورّد للبيانات	نعم	**لا شيء**
التدقيق / SIEM	يتحكم به المزوّد	**سجلاتك، SIEM الخاص بك**
الهوية	حسابات المزوّد	**Active Directory الخاص بك**

سيجمكس — المملكة العربية السعودية
7229 — حي الملك عبدالله المالي
طريق الابتكار · 3004 — حي العقيق
13519 — الرياض، المملكة العربية السعودية

السجل التجاري / الرقم الموحّد
7054521799

الرقم الضريبي
314836510700003

الموقع الإلكتروني
sigmix.sa

البريد الإلكتروني
contact@sigmix.sa

الهاتف
+966 11 525 6806

احجز جلسة تقنية →