

START HERE

Data Center Thermal Resilience Assurance

How SALAR can respond when a thermal or power event threatens compute availability, workload continuity, and customer trust

Public trigger

A thermal or power event at a cloud, colocation, enterprise, or AI compute facility creates board, cooling, workload, and continuity questions.

SALAR wedge

A traceable decision layer that converts telemetry, engineering evidence, supplier data, and recovery actions into scored repair lanes.

Commercial path

Package the response as a 48-hour incident replay, 2-week assessment, 6-week pilot, and private commercial engagement.

Prepared for: SALAR Technologies LLC | Vikrant Salar, Founder & Principal

Illustrative public-safe business-development concept. No cloud provider, hyperscaler, exchange, customer, or platform endorsement implied.



The signal: thermal stress can become business disruption

Treat any public signal as a scenario trigger, not as proof - then build an evidence-based business response.

Illustrative public pattern

A data center thermal or elevated-temperature event can affect compute/storage capacity, workload latency, service dependencies, and downstream customer operations.

Why it matters

Trading, exchange, SaaS, gaming, payment, government, and AI workloads can feel infrastructure failure even when the root cause sits inside one physical facility, zone, or region.

SALAR opportunity

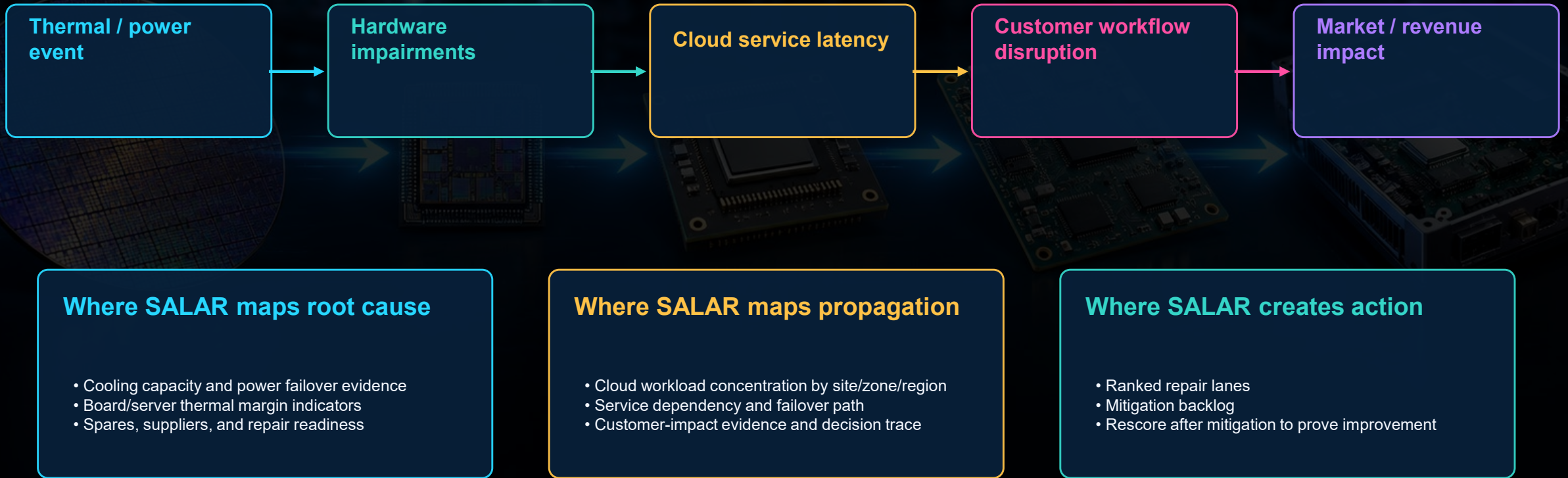
Help data center operators, cloud customers, colocation users, and AI infrastructure teams quantify thermal, workload, supplier, and failover weakness before the next visible outage.

Business-development framing: do not accuse, do not overclaim, and do not diagnose private systems. Offer a neutral “thermal resilience assurance” assessment and pilot.



The failure chain is not only cooling

A visible thermal event exposes a multi-layer reliability and continuity problem.



SALAR maps the outage into five measurable readiness pillars

Same P1-P5 doctrine, tuned for data center thermal continuity and cloud customer impact.

P1 - Thermal / Power Design

Server, rack, board, cooling path, power transfer, and thermal margin evidence.

P2 - Telemetry & Evidence Readiness

Sensor logs, cloud-health/incident events, customer-impact logs, validation artifacts, and recovery timeline.

P3 - Supplier / Provenance Intelligence

Cooling equipment, rack, server, board, spares, firmware, vendor concentration, and qualified alternates.

P4 - Operations & Process Stability

Monitoring, incident runbooks, repair cadence, re-start discipline, and controlled restoration process.

P5 - Market Continuity & Qualification

Failover tests, business/access continuity, customer communication, RTO/RPO evidence, and audit readiness.

Composite output

P1-P5 health score, gap heat map, ranked risks, decision trace, and a mitigation backlog that can be sold as an assessment, pilot, or managed service.



From fragmented signals to a repair lane

The value is not another dashboard. It is evidence-to-decision traceability.

1. Intake

Thermal logs
Power events
Cloud/zone impact
Customer workflow evidence

2. Normalize

Map data to P1-P5
Score evidence confidence
Remove noisy assumptions

3. Score

Health H_i
Gap G_i
Weighted risk
Contribution share

4. Decide

Rank repair lanes
Assign owner
Define mitigation
Rescore after action

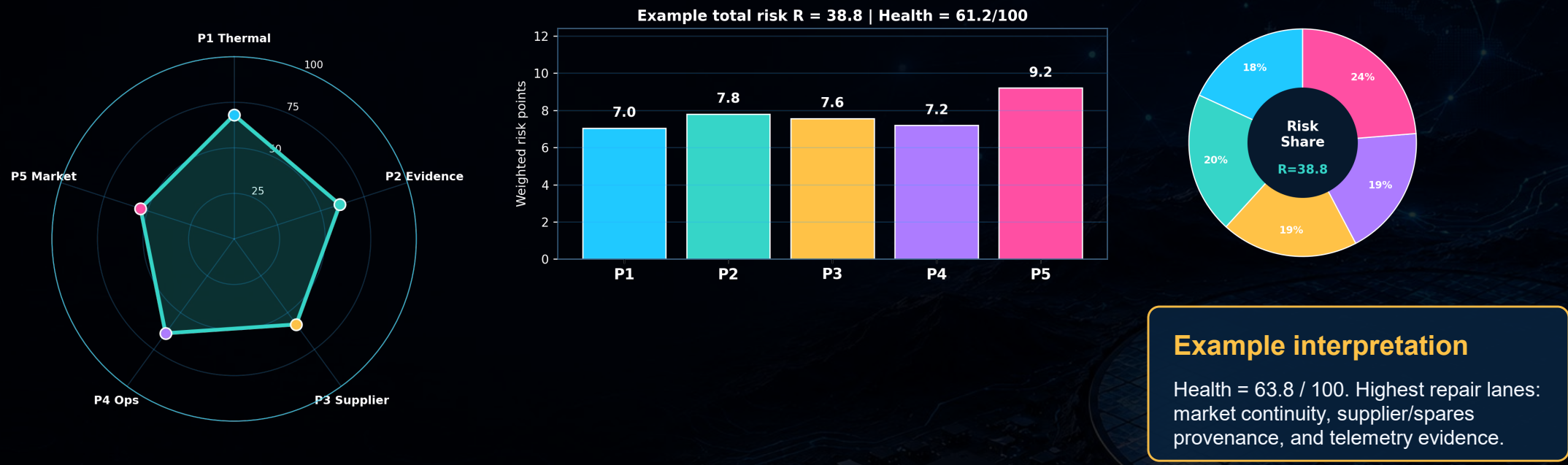
Output

A defensible narrative: what failed, how it propagated, which evidence supports the score, which repair action should happen first, and how to prove risk reduction after mitigation.



Example scoring for a thermal-event readiness assessment

Illustrative numbers only - replace with customer evidence during a paid engagement.



Formula

Gap = 100 - Health | RiskPoints = Weight × Gap | Total Risk = Σ RiskPoints | Composite Health = 100 - Total Risk



Repair heat map: where the first dollars should go

SALAR makes the repair sequence visible instead of letting every team argue from its own silo.

Gap heat map: bigger gap = first repair lane

	P1	P2	P3	P4	P5
Thermal/power	32	39	42	36	46
Cloud workload	22	30	35	28	40
Supplier/spares	18	25	32	30	38
Customer impact	20	27	36	32	44

What the heat map says

- P5 market continuity is the largest visible weakness.
- P3 supplier/spares risk is high because cooling and rack recovery depend on physical parts and service channels.
- P2 telemetry/evidence gaps slow root-cause confidence and external reporting.
- Repair sequence: evidence, failover, spares, operations, then qualification proof.

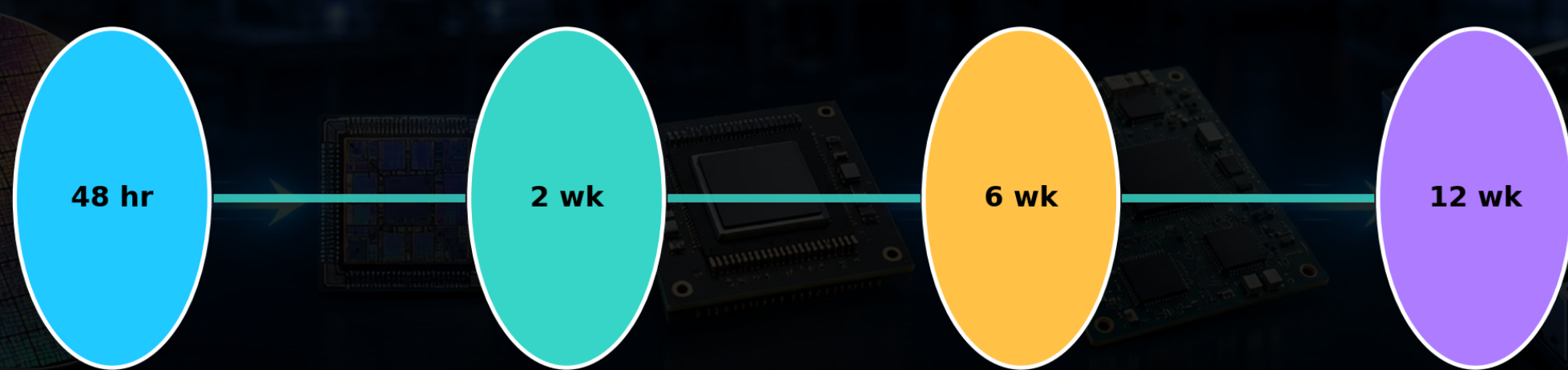
Business outcome

A buyer can fund the first engagement as an incident replay, then expand to recurring monitoring, resilience testing, and quarterly assurance scoring.



Why SALAR for thermal resilience?

A clean, productized path from scenario response to deeper assurance work.



Offer 1

48-hour public-source incident replay and executive risk memo. Scoped entry point.

Offer 2

2-week thermal resilience readiness assessment for critical compute and cloud workloads.

Offer 3

6-week P1-P5 assurance pilot with dashboard, score, heat map, and backlog.

Offer 4

12-week integration and quarterly assurance service.



SALAR Protective layer(s)

Ecosystem that works for resilience.

Primary buyer routes

- Cloud, colocation, and enterprise infrastructure teams
- AI data center / GPU-cluster operators
- Reliability, SRE, continuity, and vendor-risk owners

Impacted customer routes

- Financial, SaaS, healthcare, government, gaming, and AI workload owners
- Customer-assurance and business-continuity stakeholders
- Critical services where downtime creates revenue or trust impact

Partner routes

- Cooling, power, rack, and sensor OEM ecosystems
- Data center operators and facility engineering teams
- Observability, incident-management, and resilience partners

Thumb rule

SALAR is the assurance layer, not the cloud provider and not the cooling hardware vendor. The pitch is: “We help you know where the next thermal event could propagate and which mitigation action to fund first.”



Generic channel and route map

Public-safe channels and commercial path.

Cloud provider route

Customer account / partner channel

Critical workload resilience assessment

Cloud partner ecosystem

Co-sell / marketplace / services route

Services plus software-enabled assurance

Data center operator route

Operations / facilities / customer assurance

Thermal, power, rack, and continuity risk map

Private commercial offer route

Professional services / pilot / managed assessment

Quote only after scope and data access are clear

Cooling and power OEM route

Liquid cooling / HVAC / UPS / rack / CDU / sensors

Independent assurance and evidence-trace support

Critical workload customer route

SRE / business continuity / vendor risk / procurement

Incident replay and mitigation-priority support

SALAR contact route

salartechnologies.com/contact

Assessment, pilot discussion, and partner inquiry



How SALAR can help

Convert a thermal-risk scenario into a clear, low-friction assurance engagement that can grow.

Entry memo

48 hours

Scoped privately

Public-source incident replay + opportunity/risk brief

Rapid assessment

2 weeks

Scoped privately

P1-P5 scoring, evidence intake, heat map, action backlog

Pilot package

6 weeks

Scoped privately

Dashboard, decision trace, stakeholder readout, mitigation roadmap

Integration

12 weeks

Scoped privately

API/dashboard integration, quarterly scoring, resilience governance

Closing the first sale

Ask for one scoped 2-week assessment. Keep pricing private and quote after data access, decision owner, and deliverables are confirmed.

