

{OSIRIS}

Under your control.

MCP optimized.

Turn
Your

Portable.

AI ready.

Open.

Vendor neutral.

IT/OT infrastructure
data

The data exists. The shared picture does not.

A CIO needs reliable evidence before a decision.
An Architect needs to explain the solution.
Operations needs to troubleshoot safely.
Security needs audit-ready proof.

Each team opens a different portal, export, spreadsheet, diagram, or memory.

The result is a repeated cost pattern:

Organizations often pay repeatedly to understand infrastructure data they already own.

**Sources × Consumers
=
repeated custom translation**

Every cloud, device, controller, or platform has its own language model.

Every downstream tool needs the same truth, but has to rediscover every time it differently.

OSIRIS is a neutral infrastructure interchange layer.

OSIRIS JSON is an open specification for describing infrastructure resources, metadata, topology relationships, groups, and provider provenance in a portable JSON document.

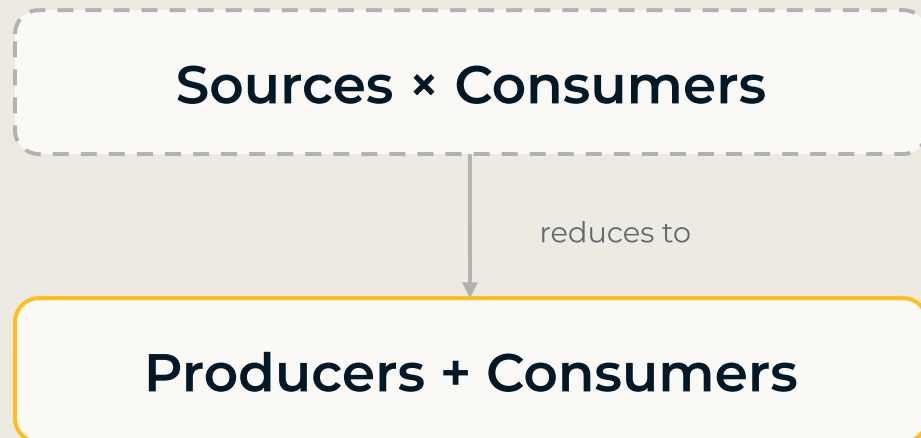
It is designed to sit between infrastructure sources and the tools that need to understand them.

OSIRIS JSON is	OSIRIS JSON is not
A point-in-time infrastructure snapshot	A real-time monitoring platform
A vendor-neutral JSON interchange format	An Infrastructure-as-Code language
A topology and evidence layer	A live control plane
A reusable artifact for many consumers and tools	A proprietary SaaS dependency
A foundation for deterministic automation and governed AI context	An AI system by itself

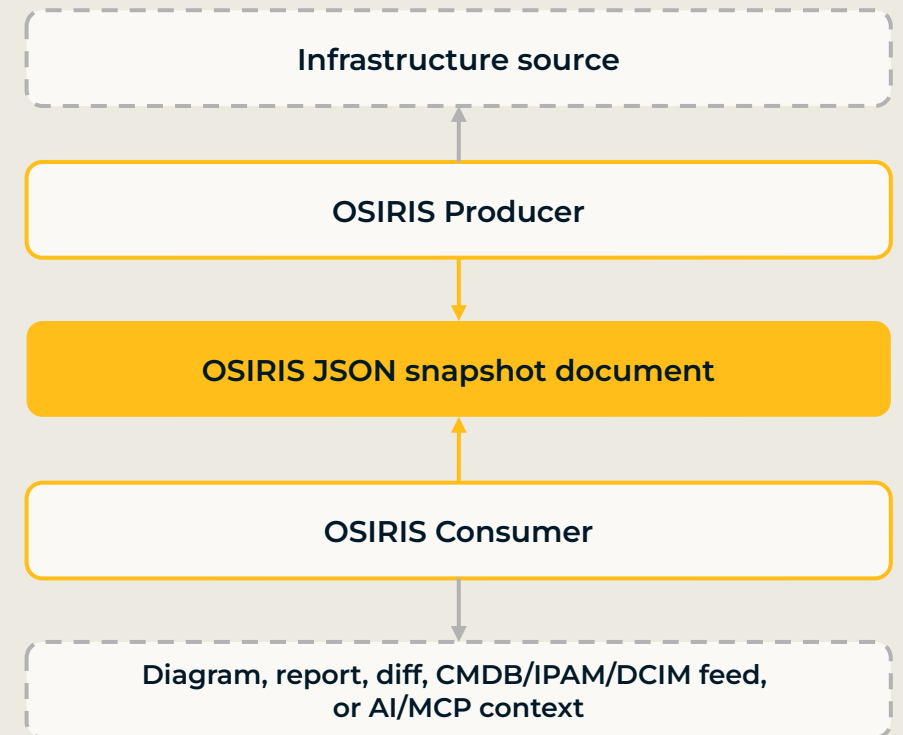
Producers translate. Consumers reuse.

OSIRIS JSON changes and improve the integration model.

Instead of forcing every consuming tool to understand every vendor language model, OSIRIS JSON creates a stable middle layer.



OSIRIS JSON build and release one producer per source and one consumer per destination.



A branch site changes over the weekend.

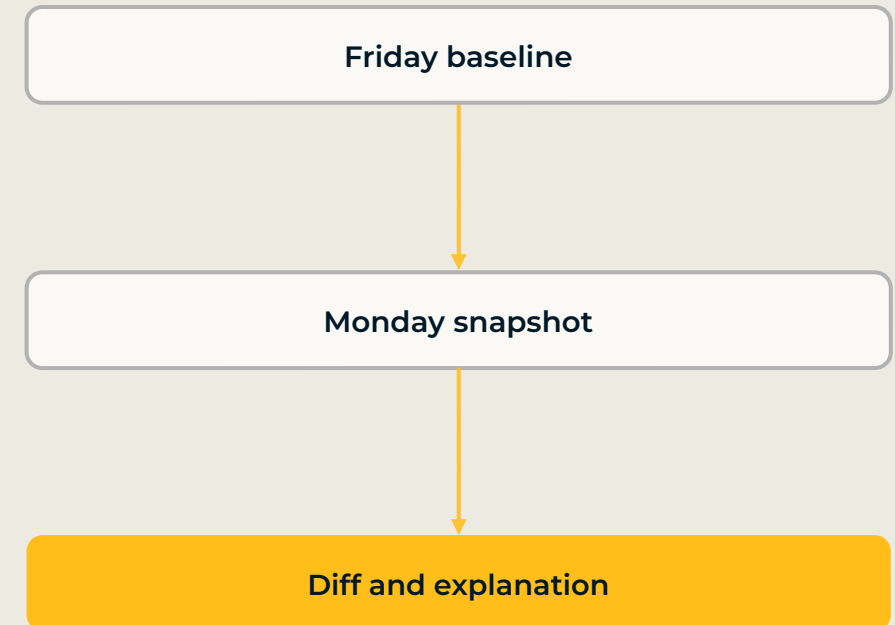
A typical use-case, on Friday, the network team generates an OSIRIS JSON snapshot for an Aruba Central site.

The snapshot captures the site topology: switches, gateways, access points, interfaces, VLANs, clients, neighbors, unmanaged devices, and health status.

On Monday, the team generates a second snapshot.

A consumer compares both documents and highlights what changed: a missing uplink, a VLAN update, a new unmanaged device, a topology difference, or a health regression.

Nobody starts from memory.
Nobody redraws the network by hand.
The investigation starts from shared evidence.

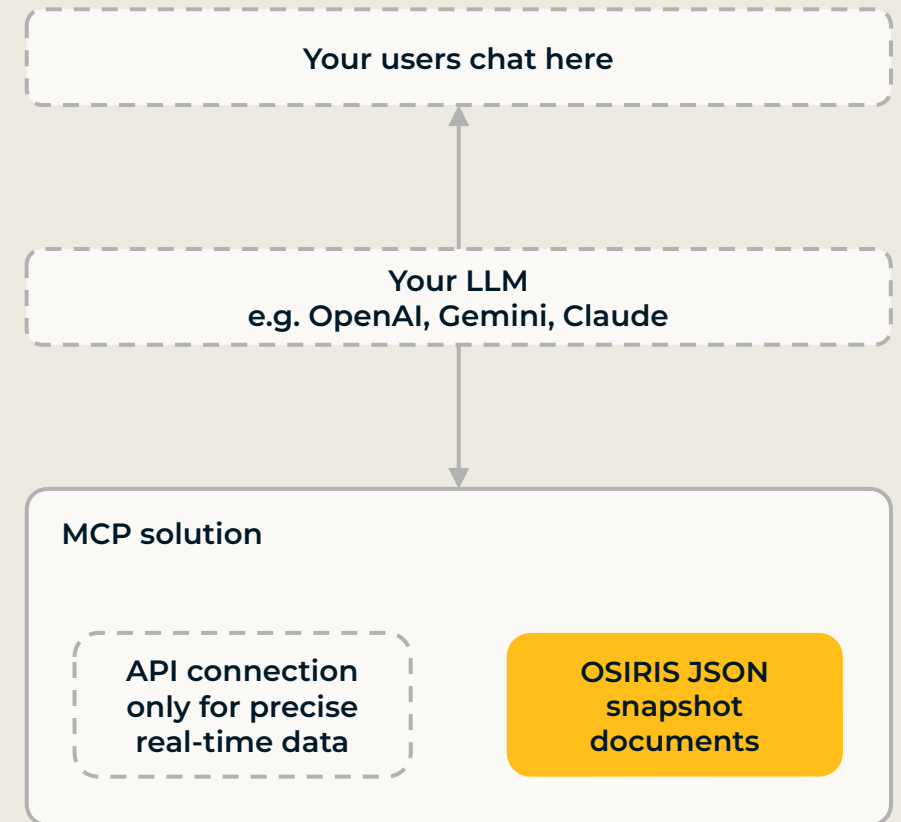


An AI MCP solution that works.

Feeding entire infrastructure configurations to an LLM exceeds context windows quite immediately, increases token costs, and risks mixing irrelevant data with critical reasoning prompts, leading to AI hallucinations.

Use OSIRIS JSON as the foundational database for a local Model Context Protocol (MCP) server. By indexing the JSON document locally, the MCP server acts as an intelligent mediator between the engineer, the local LLM, and the OSIRIS JSON infrastructure snapshot.

You don't need to connect your infrastructure to third-party solution to know your data as well as you don't have to pay "Taxes" to get access to the data you already own.



OSIRIS preserves context, not just inventory.

A flat inventory tells you what exists.
A topology snapshot tells you what it means.

The same model can describe Azure, AWS, Aruba Central,
Cisco, on-premise IT, hosting providers, and future OT extensions.

OSIRIS models infrastructure as a graph:

```
{
  "$schema": "https://osirisjson.org/schema/v1.0/osiris.schema.json",
  "version": "1.0.0",
  "metadata": {
    "timestamp": "",
    "generator": {
      "name": "osirisjson-producer-hpe-arubacentral",
      "version": "0.1.0",
      "url": "https://docs.osirisjson.org/osiris-producers/network/hpe-aruba-networking-central/"
    },
    "scope": {
      "purpose": "",
      "providers": ["hpe.arubacentral"],
      "sites": [""],
      "clusters": [""],
    }
  },
  "topology": {
    "resources": [ ... ],
    "connections": [ ... ],
    "groups": [ ... ]
  }
}
```

Resources are the things.

Connections explain how things relate.

Groups organize things by boundaries
such as subscription, VPC, subnet, site,
rack, tenant, or data center.

Metadata preserves when, how, and
from where the snapshot was
generated.

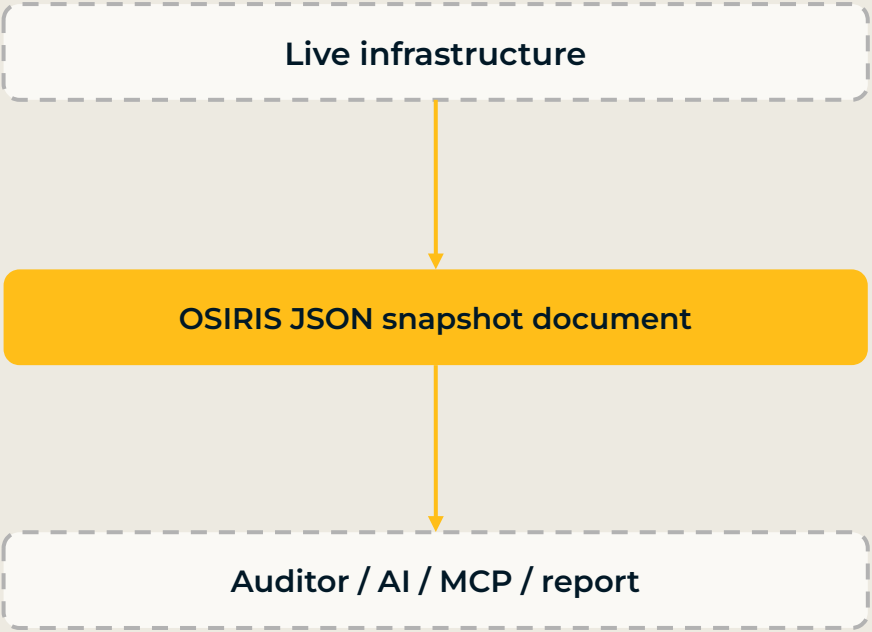
Share the artifact, not the live control plane.

OSIRIS separates understanding infrastructure from controlling infrastructure.

For governance and audit, a snapshot can become timestamped, vendor-neutral evidence that is easier to validate, archive, and review.

For AI and MCP workflows, OSIRIS provides curated infrastructure context without granting downstream tools direct access to your infrastructure.

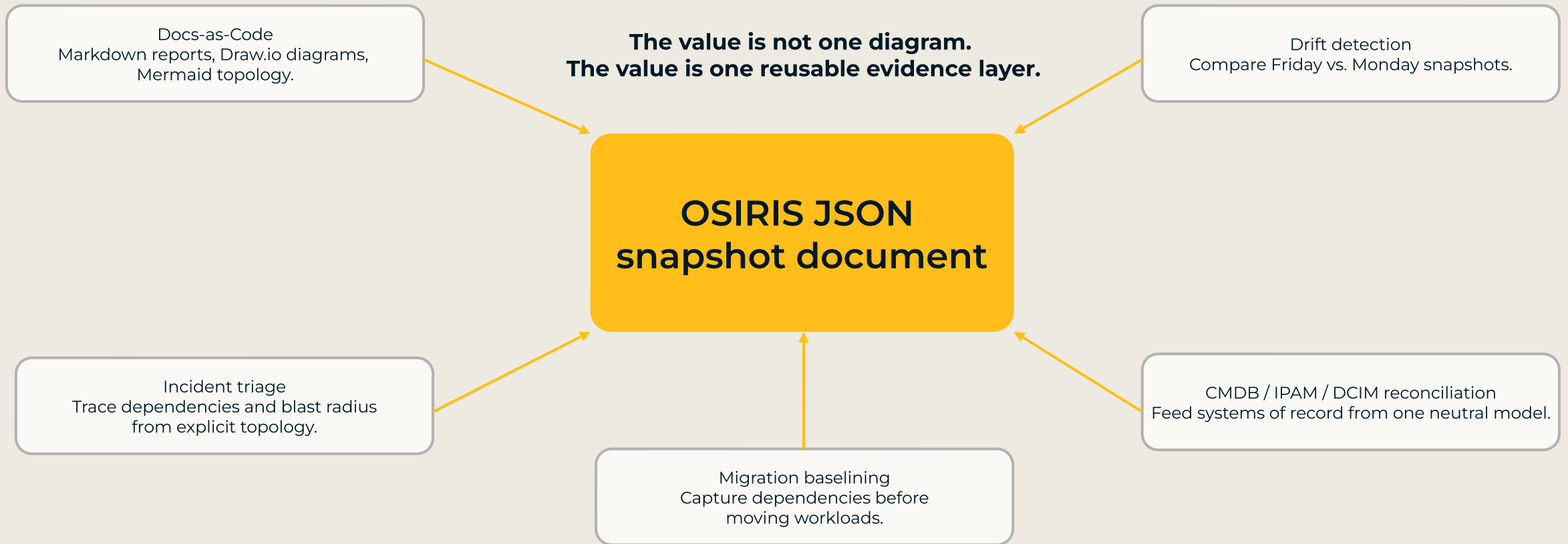
Outcome	What changes
Audit evidence	Reviewers receive a controlled artifact, not production access.
Compliance readiness	Teams can produce consistent snapshots across heterogeneous platforms.
Governed AI context	AI reasons on selected snapshot data instead of live infrastructure.
Lower hallucination risk	Reasoning is grounded in explicit resources and relationships.



Automation first. AI when useful. Always grounded in a clean snapshot.

The same snapshot supports many operational workflows.

Once generated, an OSIRIS JSON document can be reused across multiple outcomes.



Safe to pilot. Useful across roles.

OSIRIS is intentionally descriptive, not mutating.
Producers generate infrastructure snapshots; they do not provision, modify, or delete infrastructure resources.

Trust model

Trust boundary	Meaning
Read-only collection	Producers describe the current state.
Local-first execution	Run where credentials and access already exist.
Redaction at source	Secrets and authentication material are excluded before sharing.
Validation	Documents can be checked structurally and semantically.
Purpose-based output	Documentation and audit projections can carry different levels of detail.

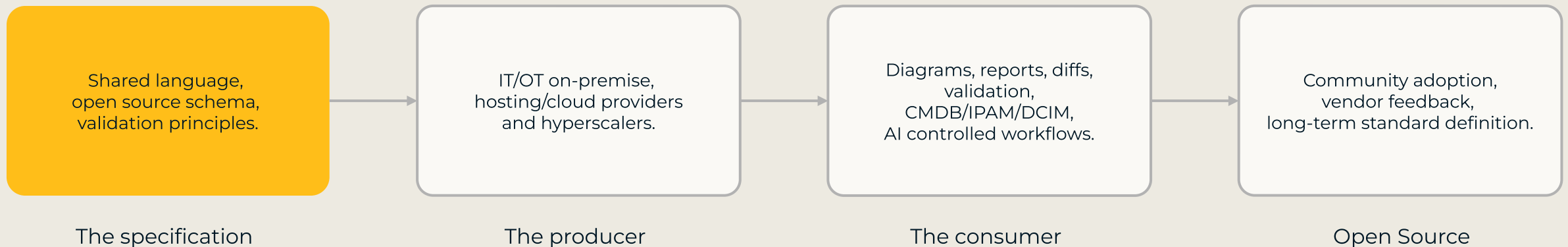
Who benefits

Role	Value
CIO / Decision maker	Better decisions from portable evidence.
Solution architect	Faster explanation of dependencies and design reality.
Operations	Faster triage and less reliance on memory.
Security / Risk	Controlled evidence without unnecessary live access.
Product owner	Reusable foundation for multiple consumer workflows.

From open specification to reusable ecosystem.

OSIRIS is more than a specification. It's a practical producer-and-consumer ecosystem.

**The OSIRIS Specification creates the language.
The OSIRIS Producers create the evidence.
The OSIRIS Consumers create the outcomes.**



Start small, prove value, then scale.

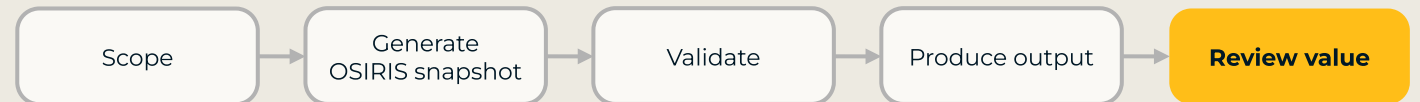
Choose one bounded environment:

- one Azure subscription,
- one AWS account,
- one Aruba Central site,
- one Cisco fabric,
- or one representative data center slice.

Recommended first outputs:

- 1) a generated architecture diagram.
- 2) a timestamped documentation or audit report.
- 3) a baseline for diff and drift comparison.

Run a low-risk proof of value:



Pilot success criteria

A current snapshot is easier to explain, safer to share, and faster to validate than today's manual documentation.

Approve one discovery-to-evidence proof of value.

OSIRIS JSON does not require a large transformation program to begin.

The first executive question is simple:

**Can we generate a trusted,
vendor-neutral snapshot of one
bounded environment and reuse it
for at least two valuable outputs?**

**One shared snapshot.
Many trusted outcomes.**

Decision requested

Approve a focused pilot with:

- One platform owner.
- One solution architect.
- One bounded infrastructure scope.
- One producer.
- Two consumer outputs.

Appendix A. Detailed use case map

Use case	Primary audience	Output
Audit evidence	CIO, CISO, risk, compliance	Timestamped vendor-neutral snapshot and report. One document for each infrastructure with end-to-end visibility.
Architecture documentation	Solution architects	Draw.io diagrams, Mermaid topology, Reports.
Drift detection	Operations, platform teams	OSIRIS document snapshot comparison and change view.
Incident triage	Operations, security	Dependency and blast-radius traversal.
CMDB/IPAM/DCIM reconciliation	Service management, platform owners	Structured feed from one neutral model.
Migration baseline	Program owners, architects	Dependency map before migration.
Governed AI/MCP	Engineering and AI platform teams	Scoped context from curated OSIRIS document snapshot as single source of truth with no requirements of connecting your infrastructure to third-party platforms.
IT/OT convergence	Infrastructure and industrial teams	Shared representation of boundaries and dependencies.

Appendix B. Documentation vs audit purpose

Purpose	Meaning	Best for
Documentation	Smaller output focused on identity, type, names, provider traceability, tags, and high-level relationships.	Diagrams, inventory views, architecture documentation.
Audit	Richer output after sensitive-field redaction, including readable properties and extensions.	Compliance review, drift analysis, deep documentation, forensic comparison.

Speaker note

Audit mode adds infrastructure detail. It does not add secrets or authentication material.

Appendix C. What OSIRIS complements

Domain	OSIRIS role	Complementary tools
Monitoring	Provides topology context, not metrics.	Prometheus, Grafana, Zabbix, OpenTelemetry.
IaC	Describes current state, not desired deployment state.	Terraform, CloudFormation, Bicep, Pulumi.
Configuration management	Documents state, does not enforce configuration.	Ansible, Puppet, Chef, Salt.
CMDB / ITSM	Feeds evidence, does not replace lifecycle workflows.	ServiceNow, NetBox, DCIM/IPAM platforms.
AI / MCP	Provides governed context, not autonomous control.	Local MCP servers, AI assistants, RAG systems.

Appendix D. Speaker narrative in 60 seconds

OSIRIS JSON exists because the infrastructure truth is fragmented across vendor languages and format, portals, APIs, tools, diagrams, and tribal knowledge.

The organization already owns the data, but every team has to translate it again for each use case: documentation, audit, drift, CMDB, migration, and now AI with agents and MCP solutions.

OSIRIS introduces a neutral layer. Producers translate source systems into a vendor-neutral JSON snapshot driven by the [OSIRIS Open Specification for Infrastructure Resource Interchange Schema](#) which is part of [JSON Schema landscape](#).

Consumers reuse that snapshot for diagrams, reports, diffs, systems of record, and governed AI/MCP context.

The important security boundary is that OSIRIS describes infrastructure; it does not control it. The OSIRIS snapshot can be generated locally, with read-only access, redacted at source, validated, archived, and shared without giving downstream tools direct live access.

The pilot is intentionally small: one bounded environment, one producer, one snapshot, two outputs. If that snapshot is easier to explain, safer to share, and faster to validate than the current manual process, OSIRIS has proven its first value.

Appendix E. Useful Links

Description	Link
The OSIRIS JSON manifesto	https://osirisjson.org/en/commitments/manifesto
The OSIRIS JSON Security Policy	https://osirisjson.org/en/commitments/security
The OSIRIS JSON Format Specification	https://osirisjson.org/en/specification
The OSIRIS JSON Core Schema	https://osirisjson.org/schema/v1.0/osiris.schema.json
The OSIRIS JSON Producer	https://docs.osirisjson.org/osiris-producers/getting-started/
The OSIRIS JSON Consumers	https://docs.osirisjson.org/osiris-consumers/getting-started/
OSIRIS JSON Use Cases	https://docs.osirisjson.org/introduction/use-cases/
GitHub	https://github.com/osirisjson

{OSIRIS}