



# BIFROST

THE AUTONOMOUS TRUST CENTER

The zero-trust gateway for agent-to-agent exchange.  
Signed answers from private data, without handing  
over the data.

**EVERY ANSWER SIGNED. EVERY REVIEW CLEARED.**

Summary

What Bifrost is

Bifrost lets one company's AI agent get trustworthy answers from another company's private data without either side handing over that data.

A requesting agent proves who it acts for. The data owner's policy decides what may be disclosed. Bifrost computes the answer inside the owner's perimeter, cites its sources, and signs it against the exact evidence it used. The requester leaves with a receipt anyone can verify. The raw records never move.

The first product built on that primitive is an autonomous trust center: the buyer's AI runs the vendor security review end to end. The same primitive applies wherever two organizations must exchange sensitive facts: insurance underwriting, M&A diligence, healthcare, legal discovery, and supply chain.

The primitive

Verified agent identity, policy before retrieval, answers instead of data, and a signed receipt for every disclosure.

The beachhead

Vendor security reviews: high frequency, painful, and already moving to AI agents on the buyer side.

The expansion

Every regulated exchange between companies where today's answer is "send us a copy of everything."

Product status: Bifrost is in active development. This paper describes the product design and the plan for expanding it. It makes no claim of existing customers or production metrics. Verticals beyond the security review are planned, not built.

01

The shift

Companies are starting to send AI agents to do work that crosses company lines. A buyer's agent reviews a vendor. A payer's agent checks a prior authorization. An acquirer's agent works through a diligence list. A procurement agent negotiates with a supplier.

Each of these exchanges needs the same four things, and today's infrastructure provides none of them:

1. **Who is asking.** Not just which API key, but which organization the agent acts for, under what agreement, and whether the token was stolen and replayed.
2. **What may be disclosed.** The data owner's rules, applied before anything is read, not a model told to be careful.
3. **An answer, not a dump.** The requester needs a fact. The owner should not have to export the database to provide one.
4. **Proof of what was said.** A record both sides, and their auditors, can verify after the fact.

Without these, companies fall back on the two options they have always had: copy the data out to the other side (data rooms, exports, shared drives) or refuse and route it to a human. The first leaks. The second does not scale to agents asking thousands of questions an hour.

## 02

# The exchange primitive

Bifrost sits at the edge of the data owner's perimeter. Every inbound question passes through the same five steps. Only the answer and its receipt leave.

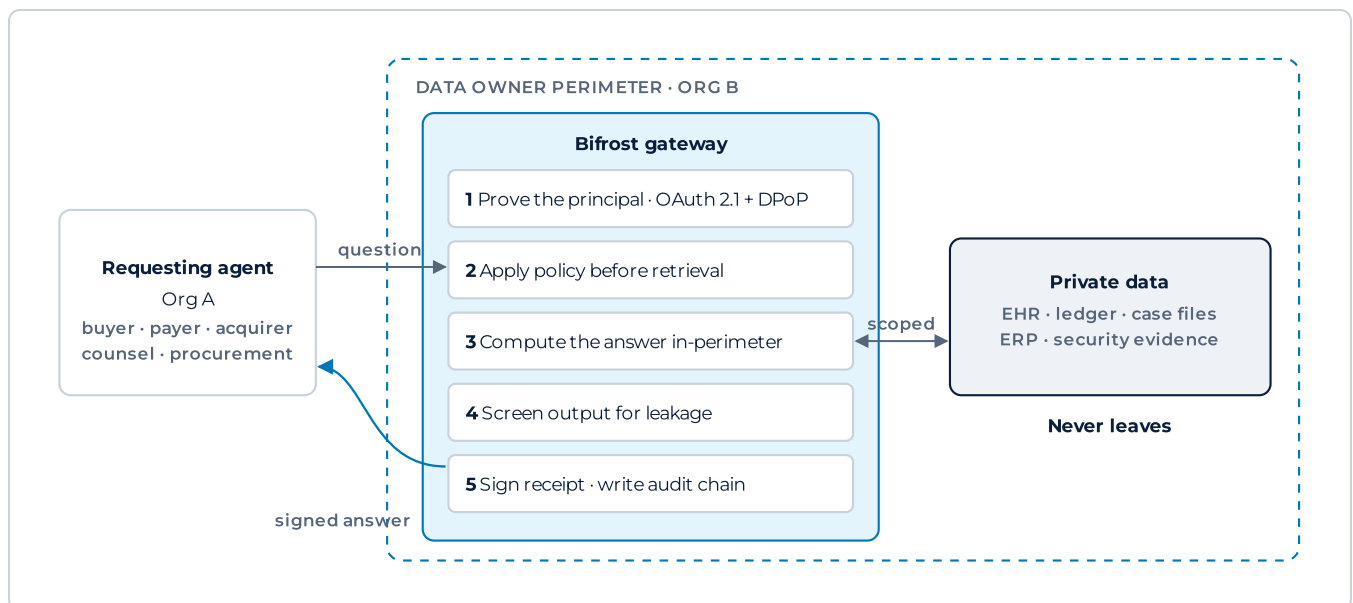


Figure 1. The exchange primitive. Questions come in, answers and receipts go out, and the raw records stay inside the owner's perimeter.

---

## 1 • Prove the principal

Agents connect over OAuth 2.1 with PKCE. Tokens are sender-constrained with DPOP, so a stolen token is useless without the agent's private key. Every request is bound to an organization, a person or system it acts for, and the agreement that governs it.

---

## 3 • Answers, not data

The answer is computed from the owner's records inside the owner's perimeter and cites its sources. If nothing supports an answer, Bifrost refuses and routes the question to a human instead of guessing.

---

## 5 • Sign and record • Differentiator

The answer is signed with the owner's key against a hash of the exact evidence used, and written to a hash-linked audit chain. The requester can verify it later, and so can their auditor.

---

---

## 2 • Policy before retrieval

The owner's rules, written in Cedar, decide what this principal may see for this purpose. Restricted material is excluded before retrieval, so the answer engine never reads what the requester is not entitled to.

---

## 4 • Screen the output

Every answer is checked for prompt-injection effects and for content above the requester's tier before it is released. Cross-tier leakage is a release-blocking test.

---

## Discoverable by any agent

A machine-readable manifest at a well-known URL tells any agent what the owner exposes, what terms apply, and how to qualify. Agents connect over the Model Context Protocol (MCP).

---

## 03

# The beachhead: security reviews

Every B2B deal of meaningful size passes through a vendor security review. The buyer sends hundreds of questions. The vendor's security lead, often one person, answers them by hand from policies, audit reports, and memory. Sales waits. Trust centers moved the documents into a portal but did not change the work, and nobody can prove an answer was true on the day it was given.

It is the right place to start. Reviews happen constantly, the pain is felt by both sides, buyers are already handing the work to AI assistants, and the data being exchanged (security evidence) is sensitive but

not regulated the way patient or financial records are. It lets the primitive harden in production before it carries higher-stakes data.

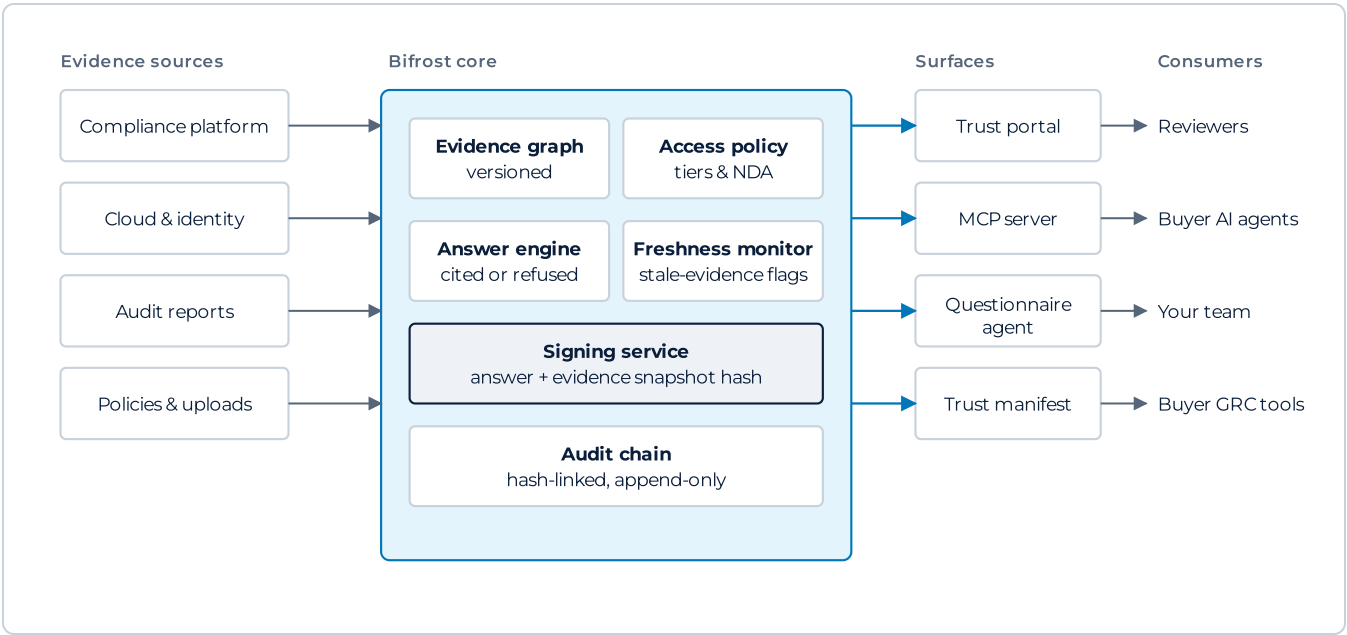


Figure 2. The trust center on the Bifrost core. Evidence enters once. Every exit enforces tier, cites a source, signs the result, and writes to the audit chain.

### Gated trust portal

Public posture, frameworks, and sub-processors, with NDA-gated and restricted tiers for reports and sensitive documents.

### Autonomous questionnaires

Upload a SIG, CAIQ, or custom spreadsheet. Bifrost answers it with citations, routes low-confidence items to you, and exports the file.

### Freshness monitor

Expiring reports and stale evidence are flagged before a reviewer sees them, and summaries regenerate when evidence changes.

### A signed answer

Each answer becomes a receipt: the question, the answer, the exact documents and versions used, a hash of that evidence snapshot, the access tier, and the vendor's signature. A verification endpoint confirms the signature and reports whether the cited evidence has since changed.

```
// Answer receipt (illustrative)
{
  "question": "Is customer data encrypted at rest?",
  "answer": "Yes. AES-256 on all production datastores; keys managed in cloud KMS with annual rotation.",
  "citations": [
    { "doc": "Encryption Policy", "version": "v4", "section": "3.2" },
    { "doc": "SOC 2 Type II Report", "control": "CC6.1" }
  ],
  "tier": "nda",
  "evidence_snapshot": "sha256:7f3c...a91e",
  "signature": "ed25519:Qm9k...Zx4=",
  "verify": "https://trust.example.com/verify/rcpt_8KQ2"
}
```

## The buyer's agent finishes the review

The buyer's agent finds the trust manifest, proves who it acts for, accepts terms, asks its questions, and leaves with a signed review packet that its own GRC tool can re-verify. Exceptions escalate to the vendor's security lead. Everything else completes with no human on either side.

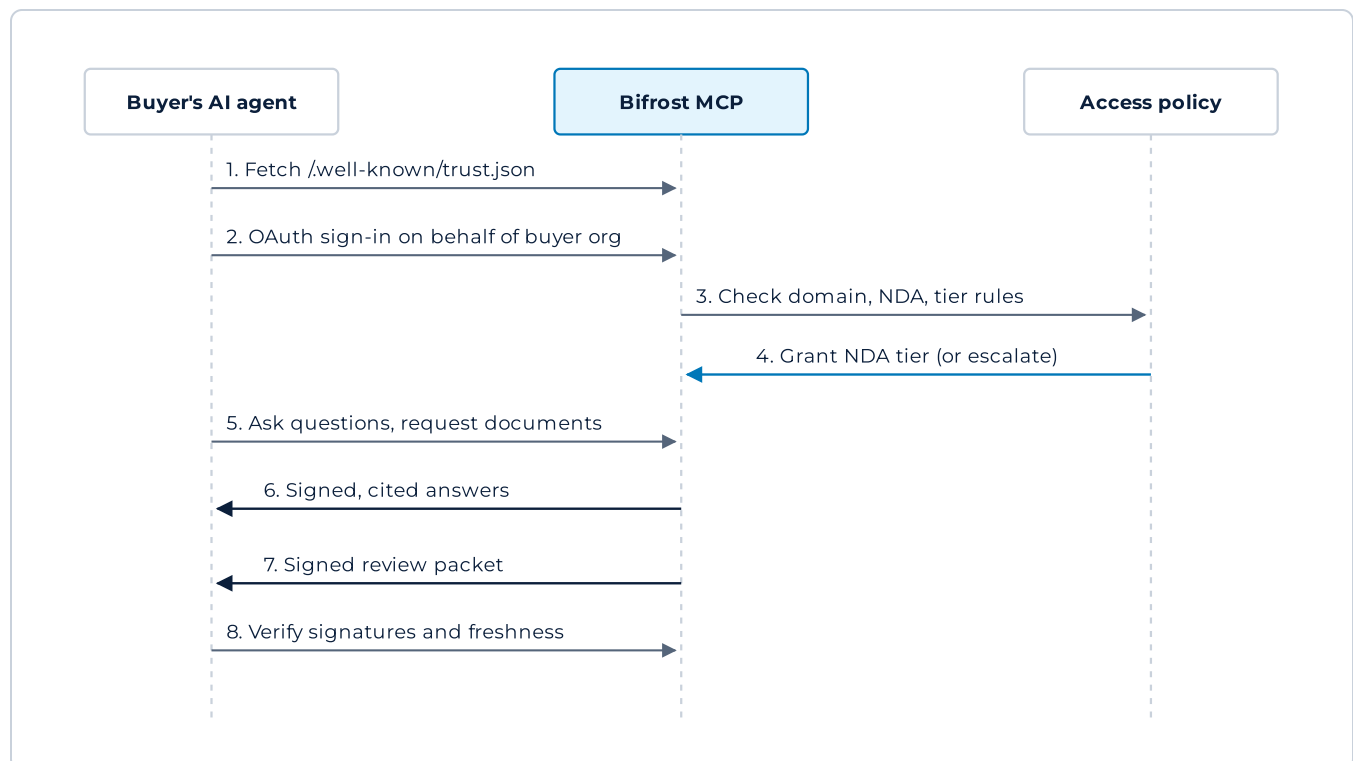


Figure 3. A complete review with no human on either side. Exceptions escalate to the vendor's security lead.

## Across verticals

Replace "vendor" and "buyer" with any two organizations that must exchange sensitive facts, and the pattern is the same. The requesting side needs an answer it can rely on. The owning side cannot hand over the underlying records, because of law, contract, or competitive risk. Each vertical below uses the same five steps. What changes is the data connector, the policy pack, and the regulation the policy encodes.

---

### INSURANCE UNDERWRITING

#### The insurer's agent verifies controls instead of reading a self-attestation

|                       |                                                                                                                                                                                               |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Today</b>          | Cyber insurers send long application forms. Applicants self-attest to MFA, endpoint coverage, and backups. Disputes surface at claim time, when the insurer finds the answer was wrong.       |
| <b>With Bifrost</b>   | The underwriter's agent asks the control questions directly. Answers come from the same evidence that backs the applicant's trust center, signed against that evidence on the day of binding. |
| <b>Never leaves</b>   | Configurations, architecture diagrams, and internal audit findings.                                                                                                                           |
| <b>Why it matters</b> | A signed, timestamped answer replaces a checkbox. Both sides know exactly what was represented at binding.                                                                                    |

---

### FINANCE AND M&A

#### The acquirer's agent audits the ledger without receiving it

|                       |                                                                                                                                                                                                                                                                  |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Today</b>          | Diligence runs through virtual data rooms. The target uploads exports of its ledger, contracts, and cap table, and loses control of them the moment they are downloaded, often to a buyer who walks away.                                                        |
| <b>With Bifrost</b>   | The acquirer's agent works the diligence list against the target's systems through Bifrost. It asks revenue-concentration, churn, and covenant questions and gets computed, cited answers. The target's policy sets what can be asked at each stage of the deal. |
| <b>Never leaves</b>   | The general ledger, customer names, and contract terms, unless the deal stage and policy allow it.                                                                                                                                                               |
| <b>Why it matters</b> | The receipts become the diligence record, and representations can point to exactly what was disclosed and when.                                                                                                                                                  |

```
// Computed disclosure (illustrative): a fact from the ledger, not the ledger
{
  "question": "Did any single customer exceed 20% of trailing-twelve-month revenue?",
  "answer": "No. Largest single customer: 14.2% of TTM revenue.",
  "computed_over": { "source": "general_ledger", "window": "TTM", "records": 48211 },
  "disclosed": ["max_customer_share"],
  "withheld": ["customer_identities", "line_items"],
  "policy": "deal_stage:loi",
  "evidence_snapshot": "sha256:c41e...07bd",
  "signature": "ed25519:Hk2w...9Lq="
}
```

## HEALTHCARE

### Payer and provider agents settle a prior authorization from the record

|                       |                                                                                                                                                                                                                                                                                                                             |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Today</b>          | Prior authorization runs on faxed and portal-uploaded chart notes. Clinical staff assemble packets by hand, payers review them by hand, and more of the record moves than the decision requires.                                                                                                                            |
| <b>With Bifrost</b>   | The payer's agent asks whether specific clinical criteria are met. Bifrost answers from the provider's record with citations to the encounters that support it, discloses only what the criteria require, and signs the answer. Deployments run in an isolated, in-region environment under a business associate agreement. |
| <b>Never leaves</b>   | The full chart, unrelated encounters, and any data that policy marks outside the minimum necessary for the request.                                                                                                                                                                                                         |
| <b>Why it matters</b> | Faster decisions, less patient data in motion, and a verifiable record of what supported each one.                                                                                                                                                                                                                          |

## LEGAL AND EDISCOVERY

### Opposing counsel's agents exchange discovery under the protective order

|                       |                                                                                                                                                                                                                                                    |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Today</b>          | Productions are bulk transfers. Confidentiality designations are stamped on documents and enforced by trust. Inadvertent production of privileged material is caught late, if at all.                                                              |
| <b>With Bifrost</b>   | The terms of the protective order and the ESI protocol become policy. Confidential and attorneys'-eyes-only designations become access tiers. Privileged material is excluded before retrieval, and requests are answered within the agreed scope. |
| <b>Never leaves</b>   | Privileged documents, and anything outside the agreed custodians, date ranges, and topics.                                                                                                                                                         |
| <b>Why it matters</b> | Each side holds a signed record of exactly what was produced, to whom, and under which designation. That record supports clawback and privilege disputes.                                                                                          |

# Procurement and supplier agents negotiate without exposing margins

|                |                                                                                                                                                                                                                                                                                                                 |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Today          | Negotiations and supplier assessments run over email and portals. Sharing enough to close a deal means sharing inventory positions, capacity, and cost structure the other side can use against you.                                                                                                            |
| With Bifrost   | The procurement agent asks, for example, whether 10,000 units can ship within 30 days at or below a target price. The supplier's policy answers yes, no, or a counter from internal systems. Compliance questions, such as origin, certifications, and software bills of materials, are answered from evidence. |
| Never leaves   | Unit costs, margins, inventory levels, and other customers' pricing.                                                                                                                                                                                                                                            |
| Why it matters | A signed quote is a record both sides can hold each other to, produced at agent speed.                                                                                                                                                                                                                          |

05

# One core, every vertical

Bifrost is not rebuilt for each market. The core that runs the security review is the same core every vertical uses. A new vertical adds a pack on top of it.

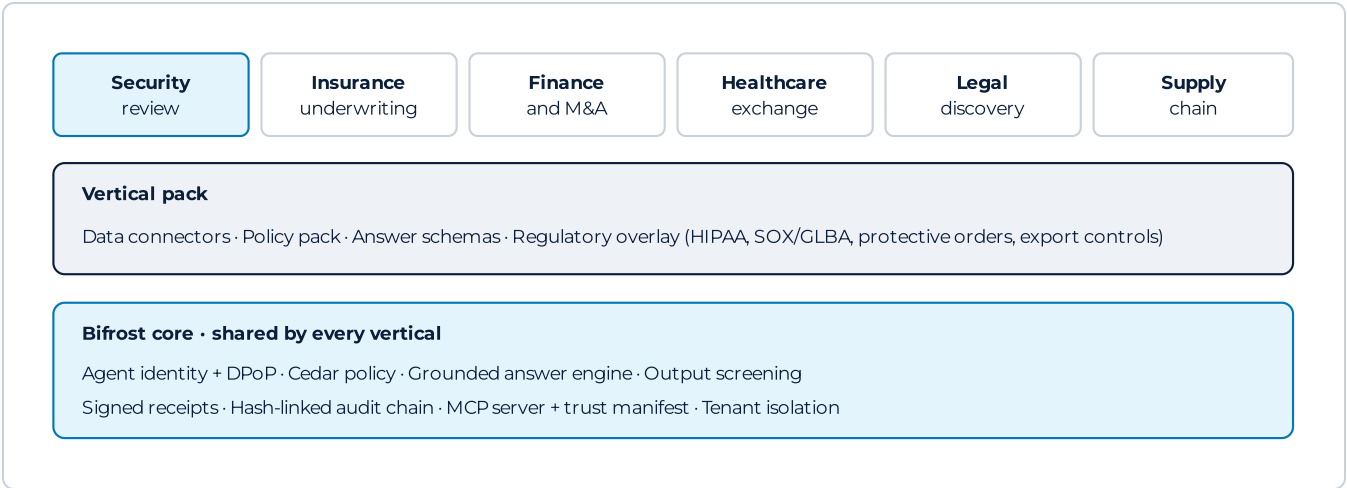


Figure 4. The security review is the first vertical, not a separate product. Each new market adds a pack, not a platform.

# Why the position compounds

**Receipts travel.** Every signed answer is verified by the party that received it. Each verifier becomes familiar with Bifrost receipts, and some will want to issue their own. A buyer that verifies vendor receipts in security reviews is a candidate to publish its own.

**Evidence is reused.** The evidence a company connects for its trust center is the same evidence an insurer or acquirer asks about. The second and third use cases cost the customer almost nothing to turn on.

**The manifest is a standard surface.** An agent that knows how to read one Bifrost manifest knows how to qualify with every Bifrost-enabled organization, in any vertical.

## 06

# Security model

A gateway that answers outside agents from private data is itself an attack surface. Bifrost is designed on the assumption that every inbound question may be adversarial.

## Two-layer access

What an agent can reach is the intersection of the scopes granted to its connection and the tier assigned to the principal it acts for. Neither layer alone is sufficient.

## Sender-constrained tokens

DPoP binds every access token to a key held by the agent. A token lifted from a log or a compromised proxy cannot be replayed.

## Refusal over invention

If no approved source supports an answer, Bifrost says so and routes the question to a human. A confident wrong answer is worse than no answer, in a security review or a prior authorization.

## Tenant isolation and keys

Row-level isolation for standard tenants. Dedicated, in-region isolated deployments for regulated data. Per-tenant encryption keys, with customer-managed keys for enterprise, and a per-tenant signing key for receipts.

## Inference inside the perimeter

The answer engine is model-portable. Standard deployments use a managed model endpoint. Isolated deployments for regulated data are designed to run inference on self-hosted models inside the data owner's environment, such as NVIDIA NIM microservices, so raw records never reach a third-party model provider.

## Containment

Rate limits per agent and per organization, a per-tenant kill switch for agent access, and a complete audit chain for incident review.

07

Business model

**Free to publish. Pay when trust clears.** In the security review, the full product is free to publish: trust portal, MCP server, signed answers, questionnaires, and agent-to-agent review. The vendor pays when a review clears: \$250 per cleared review, capped at \$24,000 per contract year. Repeat reviews from the same buyer within 90 days are free. Every paid answer carries an accuracy warranty. Enterprise plans add isolated deployment, customer-managed keys, SIEM export, and unlimited cleared reviews.

The same principle carries into each vertical: the unit of value is a cleared exchange, not a seat. Vertical pricing will be set with design partners in each market.

| Who                     | What they get                                                                                                                  |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Data owner              | Answers outside parties without exporting records. A signed record of every disclosure. Hours of manual response work removed. |
| Requesting party        | Answers it can verify instead of trusting, delivered at agent speed, with no data to secure after the fact.                    |
| Auditors and regulators | A tamper-evident trail of who asked what, under which policy, and what they were told.                                         |

08

Roadmap

Built in the current development build: signed answer receipts, the remote MCP server, the questionnaire agent, rule-based access grants, freshness monitoring, the trust manifest, delegated review packets, bulk receipt verification, signed webhooks, and SIEM export. Production deployment and design partners come next.

---

## 01 Security review

Launch the trust center on the exchange primitive with a design-partner cohort, after third-party penetration testing. Bifrost's own trust center runs on Bifrost.

---

## 02 Adjacent assurance

Cyber insurance underwriting and third-party risk programs. Same evidence, new requesters.

---

## 03 Deal exchange

Ledger, billing, and contract connectors and a diligence policy pack for M&A and financing.

---

## 04 Regulated exchange

Healthcare and legal policy packs on isolated, in-region deployments with in-perimeter inference.

---

## 05 Open verification

Publish the manifest and receipt-verification specifications so any agent or GRC tool can verify a Bifrost receipt.

### About

## Odingard Security

Odingard Security builds security and assurance infrastructure for AI-driven operations, including runtime enforcement for AI agents, autonomous red teaming, and AI-native compliance operations. Bifrost applies that work to the moment trust is decided between two companies.

---

**Odingard Security**, a Six Sense Enterprise Services company  
[andre.byrd@odingard.com](mailto:andre.byrd@odingard.com)

Bifrost is in development. Features, verticals, and packaging described here are planned and may change.