INGESTION & DISCOVERY — LAYER 1

L1 The Boundary Layer

WHERE THE PLATFORM MEETS THE OUTSIDE WORLD

L1 is the edge of Converge360 — the point where everything outside your environment becomes something the platform can reason about. It performs two jobs at once: it **brings the known in** through vendor-agnostic connectors, and it **uncovers the unknown** through active outward scanning. Both motions feed clean, normalized raw material upward to the Foundation layer.

WHERE L1 SITS

- L5 Experience
- L4 Operations
- L3 Intelligence
- L2 Foundation
- **L1 Ingestion & Discovery**

COMPONENTS
2
EdgeBridge & Discovery Tools working as one boundary.

CONSUMES
External & unknown
Third-party systems and the network estate.

PRODUCES
Raw, normalized signal
Normalized feeds and discovered raw candidates.

FEEDS INTO
↑ L2
Foundation resolves it into canonical entities.

Two components, one boundary

01

EdgeBridge

THE INTEGRATION BOUNDARY

Vendor-agnostic connectors pull from the security and cloud tools you already run — across files, APIs and protocols — normalizing them into a single raw platform feed.

02

Discovery Tools

FINDS THE UNKNOWN

Active outward scanning of the network surfaces the servers, devices, databases and infrastructure you never knew you had — and probes their open ports and services.

Why the boundary matters

L1 sets the ceiling for everything above it: the platform can only reason about what this layer brings in or uncovers. So the boundary is built to be both **exhaustive** and **disciplined** — exhaustive, so no feed or asset slips past unseen; disciplined, so whatever passes upward is already clean, consistent and ready to use. Get the boundary right and every layer inherits a complete, trustworthy picture. Get it wrong and the blind spots compound all the way to the top.

Vendor-agnostic by design
Connectors meet your tools where they are — across formats and protocols. No rip-and-replace, no waiting.

Known and unknown
Integration brings in what you run; discovery uncovers the infrastructure you don't. One layer, no hiding places.

Normalized at the door
Every source is cleaned into one consistent schema before it climbs — so every layer above inherits order.

COMPONENT 01 · INGESTION

EdgeBridge

External integration — the platform's connector boundary

EdgeBridge is the integration boundary. It **connects to what you already run** — no rip-and-replace.

Most organizations already own a wall of security and IT tooling, but the signal is trapped in a dozen vendor formats. EdgeBridge dissolves that fragmentation. Vendor-agnostic connectors reach your systems through whatever they speak — flat files, APIs, directory and shell protocols — and normalize every heterogeneous source into a single, consistent raw platform feed that every layer above can read. EdgeBridge consumes external third-party systems and produces raw, normalized feeds — the disciplined entry point for everything Converge360 does.

KEY CAPABILITIES

Vendor-agnostic connectors
A broad connector library across security and IT domains — Triquetra adapts to your stack, not the reverse.

Normalization to one schema
Every source is mapped to one consistent raw feed, so downstream layers never touch vendor quirks.

Continuous ingestion
Streaming and scheduled pulls keep the platform's view live as upstream systems change.

Resilient & secure
Managed authentication, rate-limit handling and retries keep integrations stable across flaky endpoints.

HOW EDGEBRIDGE CONNECTS

FILES · APIS · PROTOCOLS

- CSV
- XLS
- API
- LDAP
- SSH
- CSH
- CLI
- PDF
- + many more

INBOUND DATA SOURCES IT INTEGRATES

15 SECURITY DOMAINS

Vulnerability & Patch Mgmt	Threat Detection & Monitoring	Incident Response & Mgmt	Network Security	Endpoint Security
Cloud Security	Data Security & Privacy	Application & Software Security	Governance, Risk & Compliance	Third-Party / Supply Chain Risk
Security Awareness & Human Risk	Business Continuity & DR	SecOps & Program Metrics	Threat Intelligence	Email & Collaboration Security

← CONSUMES

- External third-party systems across 15 security domains
- Files, APIs, directory & shell protocols

→ PRODUCES

- Raw, normalized platform feeds in one schema
- Live input to L2 Foundation

COMPONENT 02 · DISCOVERY

Discovery Tools

Active outward scanning — finds unknown infrastructure

You cannot protect what you cannot see. Discovery Tools **surface the infrastructure nobody told the platform about.**

EdgeBridge ingests the systems you already know you own. Discovery Tools tackle the opposite, harder problem: the infrastructure that never made it onto an inventory. Through active outward scanning of the network, this component finds servers, network devices, databases, desktops and laptops, and other connected infrastructure — then probes each one, mapping the open ports and running services it exposes. The result is a stream of discovered raw candidates: newly seen infrastructure that flows upward, where Foundation decides whether each one becomes a trusted asset.

KEY CAPABILITIES

Server & endpoint discovery
Detects live servers, desktops and laptops on the network — managed or not.

Network device discovery
Surfaces routers, switches, firewalls and appliances attached to the network.

Database & infra discovery
Finds databases and other infrastructure running quietly on the estate.

Open port & service scanning
Probes each discovered host to map exposed ports and the services behind them.

WHAT IT SURFACES

- **Servers & hosts**
- **Network devices**
- **Databases**
- **Desktops & laptops**
- **Open ports**
- **Running services**

The complement to EdgeBridge

EdgeBridge sees **what is already wired in**. Discovery Tools see **the infrastructure that is not** — and probe what it exposes. Together they close the visibility gap that leaves most programs blind to a meaningful slice of their own estate.

← CONSUMES

- Networks (internal & external)
- Connected infrastructure & exposed services

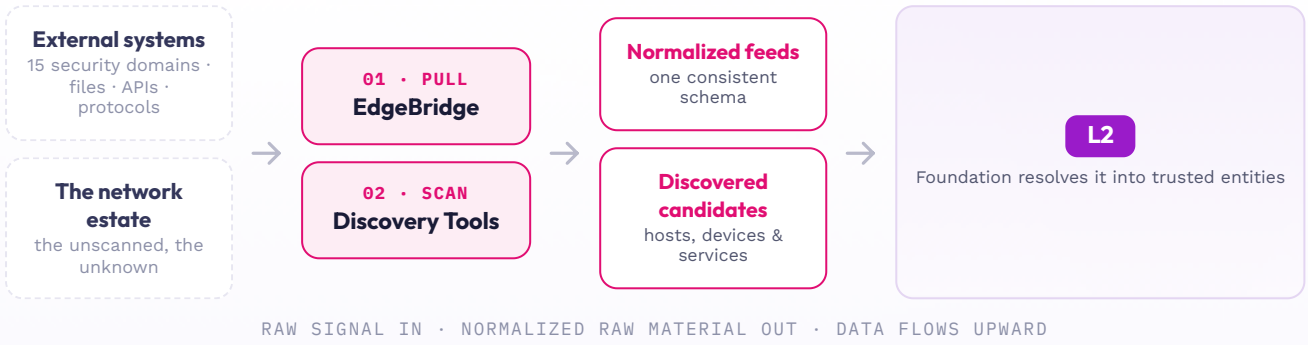
→ PRODUCES

- Discovered raw candidates — hosts, devices, databases
- Open-port & service findings for L2

HOW L1 WORKS AS ONE BOUNDARY

Two motions in, one clean signal out.

EdgeBridge pulls the systems you know about; Discovery Tools find the infrastructure you don't. Both run continuously and hand their output to the same place — giving Foundation a complete, normalized picture to build canonical entities from. Nothing reaches the rest of the platform without passing through this disciplined edge first.



CROSS-CUTTING · AGENTIC AI / LLM FABRIC

Intelligence is present at the edge — not bolted on later.

The agentic fabric threads through all five layers, including this one. At L1 it helps **enrich and de-noise incoming feeds** and **triage discovered candidates** the moment they appear — so the signal handed upward is already cleaner, richer and easier for Foundation to resolve.

COMPONENT	CONSUMES	PRODUCES	DOWNSTREAM
EdgeBridge	Third-party systems across 15 domains	Raw, normalized platform feeds	→ L2
Discovery Tools	Networks & connected infrastructure	Discovered candidates · port & service findings	→ L2

No blind spots

Known systems and unknown infrastructure are captured by the same boundary — visibility is complete from the first layer.

No rip-and-replace

Vendor-agnostic connectors mean Converge360 works with the stack you already own, on day one.

A clean foundation

Normalized, pre-triaged signal gives every layer above a trustworthy base to reason on.

EdgeBridge delivers vendor-agnostic integration — Triquetra connects to what you already run.