SYNAPSE-EDGE

ENDPOINT DETECTION & RESPONSE

OBSERVE AND CONTAIN

Endpoint detection and response that stays useful when the network does not.

Synapse-Edge collects process, network and system telemetry from every endpoint, matches it against cached threat intelligence on the host itself, and gives responders one-click containment. Detection and enforcement continue on the endpoint whether or not the management plane is reachable.

CORE CAPABILITIES

Telemetry

Process executions, outbound sockets and system events, collected by diff so a quiet host stays quiet.

Detection

IOC matching against locally cached intelligence, with a confidence floor applied at the agent to cut alert fatigue.

Response

Host isolation and hash-verified process termination, issued from the console or through Synapse-iRespond.

WHY IT IS DIFFERENT

Offline enforcement is the default, not a fallback

The agent writes its policy bundle to disk atomically and loads it before any network call. A host that boots with no connectivity still detects and still contains, against the last intelligence it received.

Containment cannot strand the host

Isolation installs the gateway allow-rules before the default-drop, and rolls back a partial ruleset on failure. An isolated endpoint always retains the path needed to receive its own release command.

Process termination is surgical

A kill order carries both PID and image hash. The agent re-hashes the running image and refuses on mismatch, so a recycled PID can never cause the wrong process to be terminated.

A footprint you do not have to tune

Interval collection with change-diffing, memoised image hashing, and constant-time detection lookups. The agent links no third-party code.

Built for an ecosystem, not an island

Synapse-Edge ships with Modular Control: a manifest pushed from your local Synapse-Gateway that reshapes the product to fit how it is deployed. One flag, one deterministic outcome.

DEPLOYMENT MODES

MODULE	STANDALONE	INTEGRATED	DELEGATED TO
In-app audit logging	Enabled	Disabled	Synapse-Cortex
Local alert console	Enabled	Disabled	Synapse-Cortex
Console response buttons	Enabled	Disabled	Synapse-iRespond
Telemetry forwarding	Disabled	Enabled	Synapse-Cortex
API-driven response	Disabled	Enabled	Synapse-iRespond
Service-quality endpoint	Disabled	Enabled	Synapse-Conectiv

The mode is enforced at the API, not merely reflected in the interface. A disabled surface returns a status naming the system that now owns it, so the console explains why a control is absent instead of appearing broken.

SECURITY POSTURE

Identity

Role-based access in the schema itself. Super Admin, Security Analyst and Service Delivery Manager, with deny-by-default checks on every route.

Multi-factor

TOTP with two-phase enrolment, single-use codes and optional global enforcement.

Hardening

Distroless non-root runtime, read-only containers, all capabilities dropped, database on an internal network.

ASSET IDENTITY

Every endpoint carries a unique asset ID anchored to its primary MAC, so a rebuilt or renamed machine resolves to the same asset instead of duplicating. Where Synapse-Cortex is connected, its asset ID takes precedence automatically — the ecosystem keeps one system of record.

AT A GLANCE

Management plane	Docker Compose: gateway, console, PostgreSQL 16
Gateway	Go, static binary on a distroless non-root image
Endpoint agent	Go, no third-party dependencies; Windows and Linux
Console	React single-page application, self-hosted, strict CSP
Telemetry	Process, network and system events
Response	Isolation, release, hash-verified process termination
Integrations	Synapse-Cortex, Synapse-iRespond, Synapse-Conectiv
Enrolment	Single-command deployment; endpoints seed automatically

Synapse-Edge is self-hosted. Telemetry, intelligence and credentials stay on infrastructure you control.