SELECTOR

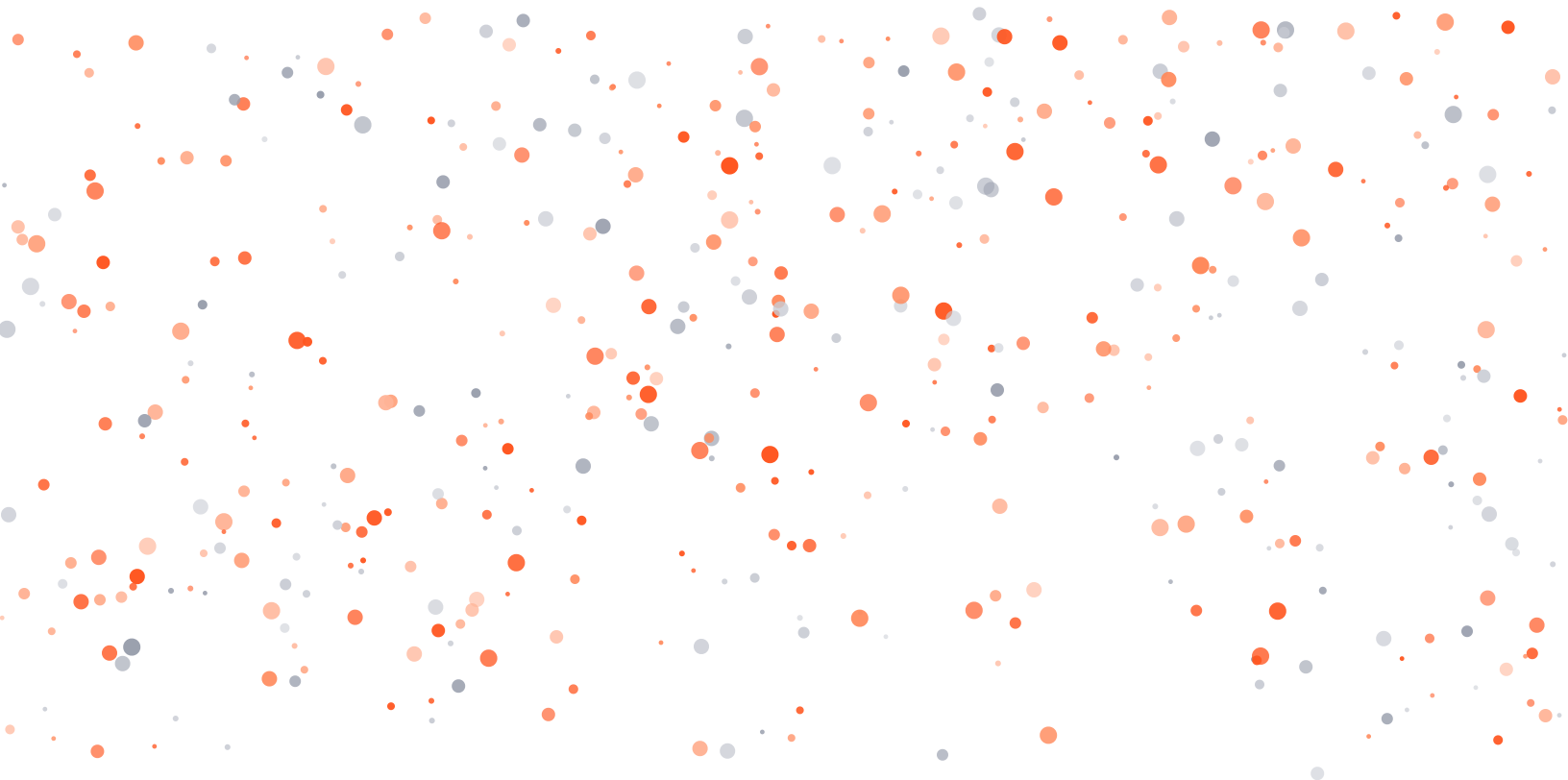
WWW.SELECTOR.AI

Technical Comparison

Selector **vs.** LogicMonitor

Observability and Event Intelligence Use Cases

October 2026



How Each Platform Builds Operational Context

Selector collects raw telemetry and operational context together from every vendor, normalizes and enriches it before any model runs, and establishes causation with purpose-built ML before agents act. LogicMonitor monitors infrastructure through collectors and LogicModule templates in LM Envision, then applies Edwin AI to the resulting alerts and events, using its ITOps Context Graph to correlate them and support investigation.

Selector

Foundry agents	Rosetta, Loom, TicketMaster, Artist, Herald, Sculptor; MCP and A2A.
Collaboration	Natural language, dashboards, ChatOps, ITSM workflows, query-backed APIs.
Knowledge	Anomaly detection, correlation, causation, forecasting, knowledge graph.
Data Hypervisor	ML schema inference, enrichment, ELT raw preservation, routing.
Collection	Horizontal engines near the source; push and pull; independent scaling.
Sources	Any vendor's devices, cloud, CMDB, IPAM, ITSM, tools, and files.

LogicMonitor

Edwin AI agents	Investigation, domain agents, workflows; Slack, Teams, ServiceNow, CLI; read-only MCP.
Event Intelligence	Alert correlation, deduplication, enrichment, AI summaries, ITSM sync.
ITOps Context Graph	Alerts, metrics, logs, topology, tickets, changes, runbooks, incident history.
LM Envision	Metrics, LM Logs, topology, dashboards, Service Insights.
Collectors	Collectors run LogicModule templates; OpenTelemetry collectors.
Sources	3,000+ integrations, Catchpoint, third-party alerts via integrations, webhooks, SDK.

Where LogicMonitor falls short architecturally:

- **Correlation centers on alerts and events:** Edwin AI ingests metrics, logs, traces, and tickets, but its correlation is organized around alerts and events from thresholds and third-party tools. Selector models raw telemetry directly, so anomalies join an incident whether or not a tool alerted.
- **Correlation, not causation:** Edwin AI clusters alerts by time, text, embeddings, and topology and surfaces probable cause. Selector orders cause and effect with deterministic topology and domain models.
- **Template-driven collection, SaaS-only platform:** LogicModules define what is collected and parsed and must be maintained; the platform is SaaS. Selector learns structure from data and deploys as SaaS, on-premises, or air-gapped.

Copyright Selector Software, Inc.

USE CASE 1: OBSERVABILITY

Multivendor Data Collection

Both platforms collect broadly. LogicMonitor is strong in infrastructure, cloud, and digital experience coverage. Selector adds network-native depth: streaming telemetry, BMP and IGP routing analytics, and context sources with no API.

DATA TYPE	SELECTOR	LOGICMONITOR
Metrics	SNMP, gNMI and model-driven streaming telemetry, Prometheus-compatible sources, REST APIs.	SNMP, WMI, APIs, and scripts through LogicModules; OpenTelemetry metrics. **Native gNMI streaming not described.**
Logs	Syslog from any device, infrastructure, or application, structured by ML; Splunk, Logstash, TACACS.	LM Logs: syslog, Windows events, application logs, and OpenTelemetry logs, with log anomaly detection.
Flow	NetFlow, sFlow, IPFIX from devices or collectors, enriched with application, owner, and criticality.	NetFlow, sFlow, IPFIX, and J-Flow through collectors.
Routing	BGP, BMP/OBMP, and IGP state ingested from customer devices.	BGP monitoring with data from private collectors, peers, and global sources, including internal routing paths. **BMP and IGP ingestion not described.**
Configuration	Running and intended config via NETCONF and CLI; drift correlated with impact.	ConfigSources collect device configurations and detect changes.
Topology	From SNMP, CDP/LLDP, configuration, and telemetry, across all vendors; digital twin.	Auto-discovered topology maps and service dependencies.
Context	ServiceNow CMDB, NetBox, Nautobot, Infoblox; owner, site, circuit, criticality.	ServiceNow CMDB through the Service Graph Connector; resource properties.
Hybrid & multicloud	AWS, Azure, Google Cloud APIs, flow logs, transit gateways, VPCs, correlated with on-prem.	AWS, Azure, and Google Cloud monitoring; cloud cost signals.
Digital experience	ICMP and UDP probes, ThousandEyes, traceroute, custom tests.	Catchpoint internet performance and digital experience monitoring.
Files / streams	Kafka, CSV, Excel, Google Sheets.	**Not described in LogicMonitor materials.**

LogicMonitor gaps

- No native gNMI or model-driven streaming telemetry described.
- BMP and IGP ingestion not described; routing analytics centers on BGP.
- Collection depends on LogicModule templates for each device type and data source.

Selector value

- Streaming telemetry, flow, routing, configuration, and context from any vendor in one pipeline.
- Routing changes tied to the services they affect inside the customer's network.
- Ingestion from files and streams for data with no API.

Copyright Selector Software, Inc.

USE CASE 1: OBSERVABILITY

Data Normalization and Enrichment

Selector normalizes and enriches every signal from every source before any model runs. LogicMonitor structures data through the LogicModule that collected it and enriches alerts as they reach Edwin AI.

CAPABILITY	SELECTOR DATA HYPERVISOR	LOGICMONITOR
Schema inference	ML infers structure from free-form logs, syslog, traps, and CLI output; no parsing templates.	LogicModules define collection and parsing per data source. **ML schema inference not described.**
Entity resolution	Named-entity and clustering models group events across vendor and format variations.	Resources and instances discovered by LogicModules; Edwin AI tags and enrichment attributes.
Enrichment	Topology, dependency, owner, site, maintenance state, and criticality added before analysis.	Resource properties, CMDB data, and Edwin AI enrichment applied to alerts.
Data fidelity	ELT: raw data lands with original timestamps; transformation follows.	Metrics and logs retained per platform retention. **Raw-data replay of network state not described.**
Noise suppression	Duplicate, flapping, and irrelevant signals removed before the intelligence layer.	Alert thresholds and dynamic thresholds at collection; deduplication in Edwin AI.
Business logic	Maintenance windows, provider notices, suppression, and criticality in YAML via DevOps workflows.	Alert rules, escalation chains, and scheduled downtime.
Customization	S2ML tunes enrichment, labeling, noise rules, prioritization, and LLM output.	Custom LogicModules authored in Groovy or PowerShell; configurable Edwin AI models.
Data access	Every view is a query and can be exposed as an API endpoint; MCP server.	REST API, dashboards, and read-only MCP for Edwin AI.

LogicMonitor gaps

- Parsing and structure depend on templates and custom LogicModules that need maintenance as vendors and formats change.
- No ML schema inference across vendor and format variations described.
- Raw-data preservation for replay of network state not described.

Selector value

- Learned normalization: no parsing templates to maintain as the environment changes.
- Every signal enriched with topology, ownership, maintenance, and criticality before analysis.
- Raw records retained with original timestamps for replay and re-analysis.

Copyright Selector Software, Inc.

USE CASE 1: OBSERVABILITY

AI-Powered Operational Analytics

Selector models every time series and log stream individually and learns what normal looks like before anything is alerted. LogicMonitor detects issues primarily through thresholds and dynamic thresholds on the metrics its LogicModules collect.

CAPABILITY	SELECTOR	LOGICMONITOR
Anomaly detection	**Self-supervised, statistical, and regression models.** A model per time series, retrained every 30 minutes, with seasonality.	Static and dynamic thresholds on metrics; anomaly detection in LM Logs.
Log analysis	**Small language models.** Log semantics interpreted, clustered across vendors, and turned into structured events.	Log anomaly detection and log queries in LM Logs.
Prediction	**Forecasting and predictive models.** Capacity forecasting and optical transceiver failure prediction.	Metric forecasting. **Optical failure prediction not described.**
Service views	**Query-chain views and digital twin.** Service, site, and dependency views built from the topology model.	Service Insights and topology maps; Catchpoint experience data added to service views.
Natural language	**Rosetta.** Plain-language questions answered with every claim linked to source data.	Edwin AI in LogicMonitor, Slack, Teams, ServiceNow, and CLI.

LogicMonitor gaps

- Detection centers on static and dynamic thresholds; per-series learned baselines for every metric are not described.
- Optical failure prediction not described.
- Natural-language answers are AI summaries; source-linked evidence for every claim not described.

Selector value

- Per-series models retrained every 30 minutes detect anomalies no threshold would catch.
- Optical failure prediction and capacity forecasting before impact.
- Every answer links to the telemetry, configuration diff, or incident behind it.

Copyright Selector Software, Inc.

USE CASE 2: EVENT INTELLIGENCE

Event Correlation and Root Cause

Edwin AI Event Intelligence is a mature correlation product that ingests LogicMonitor and third-party alerts, events, and telemetry. Selector correlates alerts together with the telemetry behind them and determines cause, not just grouping.

CAPABILITY	SELECTOR	LOGICMONITOR EDWIN AI
Inputs	Alerts and the raw telemetry, logs, flow, and configuration behind them, correlated together.	LogicMonitor alerts, metrics, logs, traces, and tickets, plus third-party events from ServiceNow, Datadog, Splunk, Dynatrace, ThousandEyes, and others via integrations, webhooks, or SDK.
Correlation method	Contextual embeddings and clustering by shared devices, interfaces, IP addresses, topology, and time.	Autoclustering and alert-embedding models, topology-aware correlation through the ITOps Context Graph, adaptive re-clustering.
Noise reduction	Up to 99.9% of irrelevant noise removed before correlation.	80 to 95% alert noise reduction cited across LogicMonitor materials.
Root cause	Deterministic causation from topology and domain logic: reboot, then link failure, then BGP flap.	Probable root cause surfaced by Edwin AI investigation. **Causation method not described.**
Symptom vs. cause	Downstream effects labeled as consequences, not separate faults.	**Not described in LogicMonitor materials.**
Unalerted conditions	Anomalies in raw telemetry join incidents even when no tool raised an alert.	Pattern recognition and anomaly detection described; correlation centers on alerts and events.
Evidence and replay	Every finding links to source data; Network DVR replays past network state.	AI-generated summaries; context graph retains incident history and known fixes. **State replay not described.**

Selector example

The Loom agent resolved 214 alerts across six tools to a single fiber cut on one long-haul span, labeled routing reconvergence and cloud failover as consequences, and flagged the secondary path at 78% utilization as the next risk.

LogicMonitor community demo

In a LogicMonitor community session, Edwin AI was shown reducing 6,747 events to 71 alerts and 7 insights in a 24-hour period. The result is fewer, grouped incidents; the cause within each insight is surfaced as probable.

LogicMonitor gaps

- Correlation groups alerts; a deterministic causation method is not described.
- Correlation centers on alerts and events rather than modeling every underlying time series directly.
- Symptom-versus-cause labeling and network state replay are not described.

Selector value

- Alert floods collapse into one incident with a named cause, consequences, and next risk.
- Telemetry, logs, flow, and configuration correlated with alerts in one model.
- Every finding is traceable and reproducible with Network DVR.

Copyright Selector Software, Inc.

USE CASE 2: EVENT INTELLIGENCE

Agents, ITSM, and Governed Action

FUNCTION	SELECTOR FOUNDRY	LOGICMONITOR EDWIN AI
Investigation	**Rosetta.** Interprets plain-language intent, dispatches agents across domains, returns one cited thread.	**Edwin AI agent.** Conversational investigation on insights and alerts, in-product and in Slack, Teams, ServiceNow, and CLI.
Correlation / RCA	**Loom.** Connects time, topology, changes, and domains into one incident with a root cause.	**Event Intelligence.** Correlated insights with probable cause and blast radius.
ITSM	**TicketMaster.** Bi-directional ServiceNow sync across the lifecycle, with per-customer field mapping and incident-aware deduplication.	Bi-directional ServiceNow sync; agent-to-agent investigation inside ServiceNow.
Communications	**Herald.** Executive briefs, ops updates, and post-incident reports from the verified record.	AI-generated event and incident summaries.
Custom agents	**Sculptor.** Turns a described playbook into a governed agent with goal, tools, triggers, and approval points.	Agent Studio configures and governs vendor-built agents: which MCP tools, integrations, and capabilities they can use. **Building new customer agents not generally available.**
Action	Agents investigate, act, and verify within operator-set limits on high-confidence findings.	AI Automation finds validated Ansible, Terraform, and Rundeck workflows, generates new Ansible playbooks with IBM watsonx Code Assistant, and runs self-healing remediation that is validated before tickets close; approvals and policy controls apply.
MCP	Production MCP server with OAuth2, granular RBAC over insights, recommendations, and actions.	Read-only MCP access to monitoring context and Edwin AI intelligence.
Deployment	SaaS, on-premises, customer cloud, or air-gapped.	SaaS; collectors on-premises. **On-premises or air-gapped platform not described.**

LogicMonitor gaps

- Agent Studio configures and governs vendor-built agents; building new customer agents is not generally available.
- MCP access is read-only.
- SaaS-only platform.

Selector value

- Sculptor builds governed agents from the team's own playbooks, acting only on verified findings.
- MCP server shares insights and governed actions with other agent platforms.
- Deployment in SaaS, on-premises, or air-gapped environments.

Copyright Selector Software, Inc.

SELECTOR

Functionality Gained with Selector

Capabilities a LogicMonitor customer adds with Selector, whether Selector runs alongside LogicMonitor or replaces it.

1. Detection beyond thresholds

Per-series models find conditions no LogicModule threshold or third-party tool alerted on, and bring them into the incident.

2. Causation, not clustering

Deterministic topology and domain models name the root cause and label downstream symptoms as consequences.

3. Network-native depth

gNMI streaming telemetry, BMP/OBMP and IGP analytics from the customer's own devices, and optical failure prediction.

4. Reproducible investigations

Raw data preserved with original timestamps; Network DVR replays past network state so findings can be verified and re-run.

5. No templates to maintain

Learned normalization infers structure across vendors and formats, replacing parsing rules and custom collection scripts.

6. Your playbooks as agents

Sculptor turns the team's own runbooks into governed agents with approved tools, triggers, approval points, and audit.

7. Governed action through MCP

Selector's MCP server exposes insights, recommendations, and actions under OAuth2 and RBAC, not read-only context.

8. Deployment choice

SaaS, on-premises, customer cloud, or air-gapped, for regulated and isolated environments.

9. Custom outcomes with engineers

Forward deployed engineers build integrations, data models, views, and agents on the customer's own data.

10. No rip-and-replace

Selector ingests from LogicMonitor itself, so teams add causal root cause and governed agents above their existing monitoring.

Copyright Selector Software, Inc.

Selector Patents Driving Innovation

The techniques that define the Selector platform are covered by Selector's U.S. patent portfolio. Patent records are available on request.

CAPABILITY	WHAT SELECTOR'S PATENTED APPROACH DELIVERS
Root Cause Analysis	Deterministic causation across every domain.
Reproducible Investigations	Network DVR replays network state so an investigation can be re-run.
Log Intelligence	Structured signal from any vendor's syslog without parsing templates.
Conversational Investigation	Learns each customer's names for sites, services, and devices without manual labeling.
Custom Outcomes on Demand	Declarative query chains for drill-downs and customer-specific views.
Operational Context	Maintenance-window-aware alerting and reporting.
Optical Failure Prediction	Flags failing optics before they cause an outage.
Capacity Planning	Forecasts capacity limits before they affect services.
Scale	Efficient storage and querying of millions of data points per minute.

Copyright Selector Software, Inc.

Selector vs. LogicMonitor at a Glance

CAPABILITY	SELECTOR	LOGICMONITOR
OBSERVABILITY		
Data Collection	Any vendor, including gNMI, BMP/IGP, flow, config, and file sources.	Broad infrastructure, cloud, and DEM coverage via LogicModules and Catchpoint.
Normalization	Learned schema inference; ELT raw preservation.	Template-based collection and parsing.
Detection	Per-series models retrained every 30 minutes.	Static and dynamic thresholds; log anomaly detection.
Prediction	Capacity forecasting and optical failure prediction.	Metric forecasting.
EVENT INTELLIGENCE		
Correlation Inputs	Alerts plus the raw telemetry behind them.	Alerts and events, with metrics, logs, traces, and tickets.
Root Cause	Deterministic causation with symptom labeling.	Clustering with probable cause.
Reproducibility	Network DVR replay; source-linked evidence.	AI summaries; incident history in context graph.
Custom Agents	Sculptor builds governed agents from playbooks.	Agent Studio governs vendor-built agents; new customer-built agents not generally available.
MCP	Insights, recommendations, and governed actions.	Read-only.
Deployment	SaaS, on-premises, or air-gapped.	SaaS.

The Bottom Line

LogicMonitor is an established SaaS observability platform with broad integration coverage, strong cloud and digital experience monitoring, and a capable alert correlation product in Edwin AI.

Selector is built for a different starting point. It collects raw telemetry and context from every vendor, preserves and enriches it before analysis, determines cause rather than clustering alerts, and puts governed agents on top, including agents built from your own playbooks. Because Selector ingests from LogicMonitor, teams can add it without replacing existing monitoring.

30 min	99.9%	8x
Model retraining cycle	Noise reduction	Faster resolution per P1

See Selector on your own data

Request a Demo

www.selector.ai | sales@selector.ai

Copyright Selector Software, Inc.