SELECTOR

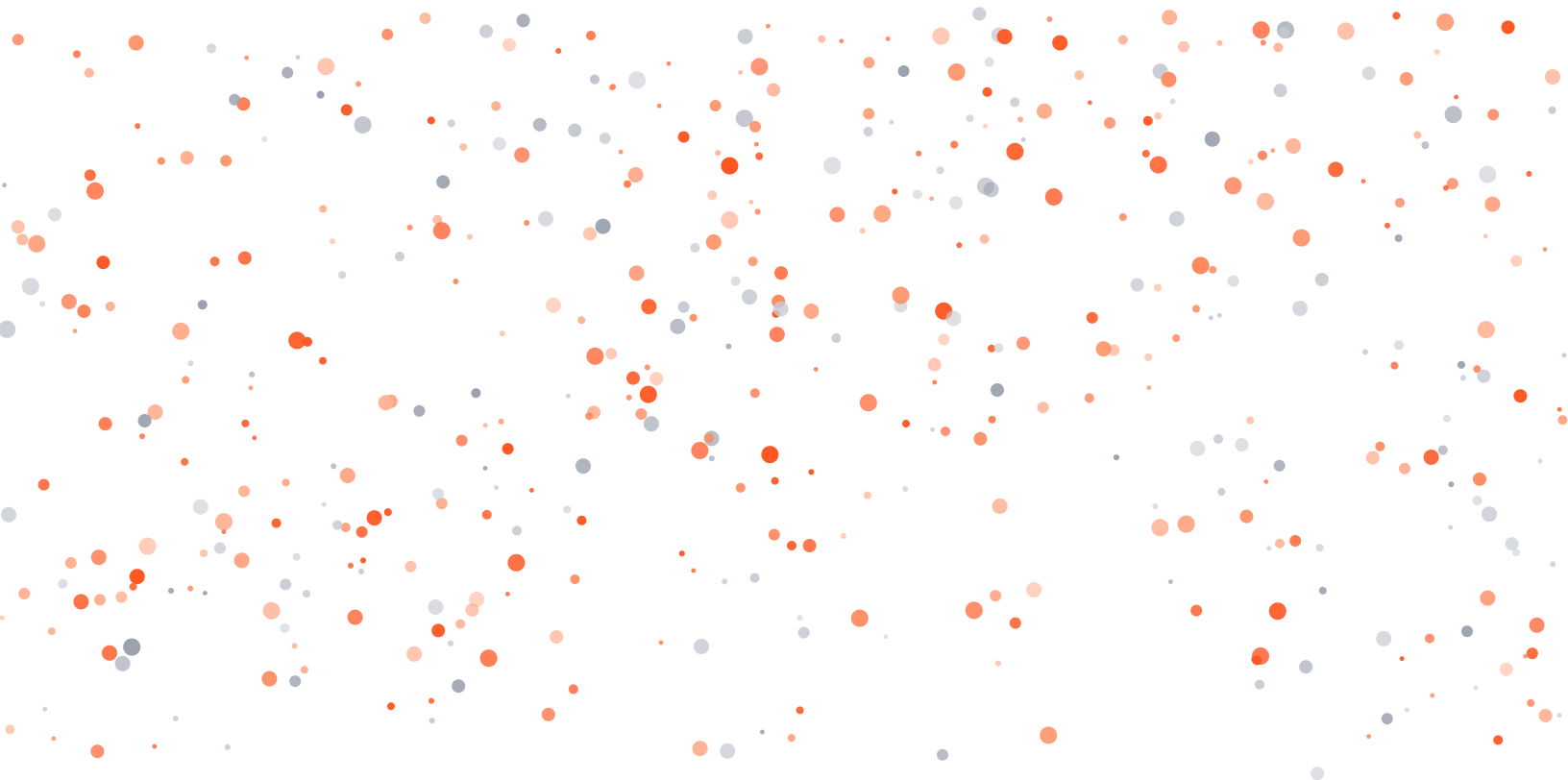
WWW.SELECTOR.AI

Technical Comparison

Selector **vs.** Cisco Cloud Control

A Technical Comparison for Operations Teams

October 2026



How Each Platform Builds Operational Context

Selector sits horizontally across every vendor and domain: it collects raw telemetry and context, normalizes and enriches it before any model runs, and establishes causation with purpose-built ML before agents act. Cisco Cloud Control is a normalized cross-product control plane for the Cisco portfolio: domain products contribute data to the Cisco Data Fabric, and shared platform services feed AI Canvas, AI Assistant, and Cloud Control Studio.

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.

Cisco Cloud Control

Agentic experiences	AI Canvas, AI Assistant, Cloud Control Studio and Agent Builder.
Platform services	Identity, tenancy, RBAC translation, assets, topology, search, audit, workflow.
Control plane	Normalized cross-product operating language for apps and agents.
Cisco Data Fabric	Normalized where correlation needs it; federated for live product context.
Domain products	Meraki, Catalyst Center, Nexus, ThousandEyes, Security Cloud Control, Webex.
Third parties	Connected through Cloud Control Studio; 50+ integrations planned.

Where Cisco Cloud Control falls short architecturally:

- **Native coverage focuses on Cisco products:** Third-party coverage depends on supported integrations. Selector collects and normalizes multivendor telemetry into one shared model.
- **Conclusions depend on LLM-based agents:** Cisco applies AI assistants and agents over shared context and evaluates their output for hallucination. Selector establishes causation with deterministic models before an LLM is involved.
- **No raw-data preservation described:** Cisco normalizes and federates data; investigations cannot be replayed against original records. Selector retains raw data with original timestamps and replays network state.

Copyright Selector Software, Inc.

Multivendor Data Collection

Selector collects telemetry and the context to interpret it in one pipeline, from any vendor. Cisco Cloud Control ingests signals from Cisco domain products and reaches other tools through connectors.

DATA TYPE	SELECTOR	CISCO CLOUD CONTROL
Metrics	SNMP, gNMI and model-driven streaming telemetry, Prometheus-compatible sources, REST APIs.	Health and performance signals from Cisco domain products.
Logs	Syslog from any device, infrastructure, or application; Splunk, Logstash, TACACS.	Events from Cisco products. **Third-party logs arrive through Splunk, which needs a separate Splunk Cloud Platform subscription.**
Events / alerts	SNMP traps, syslog-derived events, alerts from monitoring, ITSM, and observability tools.	Alerts from Cisco products, correlated and prioritized.
Flow	NetFlow, sFlow, IPFIX from devices or collectors.	**Not a Cloud Control data type.** Flow would have to land in Splunk first
Routing	BGP, BMP/OBMP, and IGP state from customer devices.	Routing events referenced in Cisco examples. **No BGP or IGP collection from internal devices.**
Configuration	Running and intended config via NETCONF and CLI; drift detection.	Compliance signals in the Unified Asset Inventory; agents check configuration against policy.
Topology	From SNMP, CDP/LLDP, configuration, and telemetry, across all vendors.	Live topology of the Cisco estate from the Unified Asset Inventory.
Context	ServiceNow CMDB, NetBox, Nautobot, Infoblox, owner, site, circuit, criticality.	ServiceNow, Infoblox, BlueCat, NetBox Labs through Cloud Control Studio connectors.
Hybrid & multicloud	AWS, Azure, Google Cloud APIs, flow logs, transit gateways, VPCs, and maintenance events, correlated with on-prem	**AWS, Google Cloud, and Microsoft integrations planned, not available.**
Synthetics	ICMP and UDP probes, ThousandEyes, traceroute, custom tests.	ThousandEyes as a converged Cisco product.
Files / streams	Kafka, CSV, Excel, Google Sheets.	**Not described in Cloud Control materials.**

Cisco Cloud Control gaps

- Collects device telemetry natively only from Cisco; no flow, BMP or IGP collection.
- Multicloud means Cisco in the cloud: security (Multicloud Defense) or Cisco-run connectivity (Multicloud Fabric, public beta). The customer's own cloud network is not an operational data source.
- Collection runs through Cisco domain products; independent collector scaling not described.

Selector value

- Collects raw telemetry, flow, routing, configuration, and context from any vendor in one pipeline.
- Integrates supported devices and tools through standard protocols, APIs, databases, or file sources.
- Deploys collectors near the source and connect outbound only; hybrid-cloud visibility without rerouting traffic through a vendor fabric.

Copyright Selector Software, Inc.

Data Normalization and Enrichment

Correlation is only as reliable as the data beneath it. Selector normalizes and enriches every signal from every source before any model runs. Cisco Cloud Control normalizes Cisco product data into shared assets, topology, and context.

CAPABILITY	SELECTOR DATA HYPERVISOR	CISCO CLOUD CONTROL
Schema inference	ML infers structure from free-form logs, syslog, traps, and CLI output; no parsing templates.	LLM-based schema transformation (Deep Network Model "LAPSE") and Splunk Auto Schematization. **Not described as an inline step for every record at ingest.**
Entity resolution	Named-entity and clustering models group events across vendor and format variations.	Unified Asset Inventory maps devices, sites and alerts across Cisco products. **AI Canvas inventory matching covers devices only, not sites or clients,** and each tenant is queried separately.
Enrichment	Topology, dependency, owner, site, maintenance state, and business criticality added before analysis.	Assets carry live operational, compliance, reachability, and vulnerability signals.
Data fidelity	ELT: raw data lands with original timestamps; transformation follows.	Hybrid model: normalized where correlation needs it, federated for live product context.
Noise suppression	Duplicate, flapping, and irrelevant signals removed before the intelligence layer.	Alerts correlated and prioritized across products.
Business logic	Maintenance windows, provider notices, suppression, and criticality defined in YAML via DevOps workflows.	Runbooks, SOPs, and policies converted into agent skills.
Customization	S2ML tunes enrichment, labeling, noise rules, prioritization, and LLM output.	SDKs, contribution contracts, agent-friendly APIs, headless modes, and CLIs.
Data access	Query backed views accessible through natural language, UI, and APIs.	Governed services consumed through UI, natural language, automation, CLI, or agents.

Cisco Cloud Control gaps

- No ML schema inference for third party logs described.
- Entity matching stops at devices: sites and clients aren't resolved, and each tenant is queried separately with no combined view.
- Customer business logic (maintenance windows, criticality) is not described as part of data enrichment.

Selector value

- Every signal is normalized and enriched before any model runs.
- Raw records retained with original timestamps for replay and re-analysis.
- Maintenance windows, ownership, and criticality applied in YAML and S2ML.

Copyright Selector Software, Inc.

AI-Powered Operational Analytics

Selector separates reasoning from presentation: purpose-built models detect, correlate, and establish causation, and language models only explain the result. Cisco Cloud Control applies AI assistants and agents over converged context and traces their activity.

STAGE	SELECTOR	CISCO CLOUD CONTROL
Signal detection	**Self supervised, statistical, and regression models; small language models for logs.** A model per time series, retrained every 30 minutes, with seasonality. Up to 99.9% of irrelevant noise removed.	Alerts correlated and prioritized across Cisco products. **Detection method not described.**
Correlation	**Contextual embeddings and clustering.** Anomalies grouped into episodes by shared devices, interfaces, IP addresses, topology, and time window.	Correlated events across products using converged telemetry, topology, and event context.
Causation	**Causation, recommender, and association models; sequential mining.** Topology and domain logic order cause and effect: reboot, link failure, BGP flap.	Cross-domain chains identified over converged context, for example workload migration, routing reconvergence, degraded Webex. **Causation method not described.**
Prediction	**Trend, forecasting, and predictive models; knowledge graph.** Capacity forecasting and optical failure prediction.	**Not described in Cloud Control materials.**
LLM role	**LLM agnostic; presentation only.** Deterministic findings translated to narrative, every claim linked to source data.	AI Assistant and agents reason over platform context; AI Canvas cards link to the prompt and context that produced them.
Reproducibility	**Raw data retained; Network DVR.** Replays historical network state so an investigation can be re-run.	Splunk AI Agent Monitoring traces LLM calls, tool use, and skills; Galileo-based evaluation scores output and flags hallucination.

Cisco Cloud Control gaps

- Detection, causation, and prediction methods not described.
- Root cause comes from LLM-based reasoning, whose output Cisco evaluates for hallucination.
- Reproducibility is limited to tracing agent activity; network state replay not described.

Selector value

- Deterministic causation from topology and domain logic; same inputs, same conclusion.
- LLM-agnostic: language models explain findings, they do not produce them.
- Network DVR replay and capacity and optical failure prediction.

Copyright Selector Software, Inc.

Data Correlation and Analysis

Selector determines root cause automatically and continuously, without static rules or thresholds, and shows the evidence for every conclusion. Cisco Cloud Control correlates events across Cisco products and relies on AI assistants and agents to investigate.

CAPABILITY	SELECTOR	CISCO CLOUD CONTROL
Correlation dimensions	Shared devices, interfaces, IP addresses, topology relationships, time window, and configuration changes.	Converged telemetry, topology, and event context across Cisco products.
Cross-vendor & cloud scope	Cisco and non-Cisco devices, carriers, interconnects, cloud-native networking, and applications in the same causal model.	Cisco domains; cloud segments only where traffic runs through Multicloud Fabric or Cisco firewalls; other data through connectors.
Root cause method	The causation model applies topology and domain logic to order cause and effect: reboot, then link failure, then BGP flap.	**Not described; investigation performed by AI assistants and agents.**
Symptom vs. cause	Downstream effects, such as reconvergence and failover, are labeled as consequences, not separate faults.	**Not described in Cloud Control materials.**
Change correlation	Configuration diffs and change events are correlated directly with degradation; drift is detected.	Agents check configuration compliance. **Change-to-impact correlation method not described.**
Impact	Upstream cause, downstream impact, affected services and owners, and the next risk are identified.	Topology shows the impact of changes and incidents on the operating environment.
Evidence	Every claim links to the telemetry, configuration diff, or incident record behind it; same inputs, same conclusion.	AI Canvas cards link to the prompt and context that produced them.
Historical analysis	Network DVR replays past network state; past incidents can be re-analyzed with current context.	**Not described in Cloud Control materials.**

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.

Cisco's published example

Cisco describes tracing degraded Webex calls through a routing reconvergence to a workload migration. That chain can only be found when every link is in the data; when one link is a non-Cisco carrier, firewall, or cloud construct, it sits outside Cloud Control's converged data.

Cisco Cloud Control gaps

- Root cause method and symptom-versus-cause separation are not described.
- Investigations are performed by LLM-based agents whose output is evaluated for accuracy and hallucination; reproducibility of a finding is not described.
- Correlation covers Cisco domains; non-Cisco links in a failure chain arrive only through connectors.

Selector value

- Deterministic, topology-aware causation across every vendor and domain.
- Alert floods collapse into one incident with a named cause, consequences, and next risk.
- Every finding is traceable and reproducible with Network DVR.

Copyright Selector Software, Inc.

Agent Orchestration and Workflows

FUNCTION	SELECTOR FOUNDRY	CISCO CLOUD CONTROL
Investigation	**Rosetta.** Interprets plain-language intent, dispatches agents across domains, returns one cited thread.	**AI Assistant and AI Canvas.** Natural-language answers; multiplayer workspace where operators and agents investigate together.
Correlation / RCA	**Loom.** Connects time, topology, changes, and domains into one incident with a root cause.	**AI Canvas sub-agents.** Dynamic sub-agents for discovery, compliance, topology, and vision analysis.
ITSM	**TicketMaster.** Creates, enriches, routes, and synchronizes tickets with impact, evidence, and owner.	ServiceNow and other ITSM tools connected through Cloud Control Studio.
Operational views	**Artist.** Builds live dashboards from a plain-language description.	AI Canvas generates UI cards for an investigation which **can't be restored after a page refresh once removed**.
Communications	**Herald.** Executive briefs, ops updates, and post-incident reports from the verified record.	**Not described in Cloud Control materials.**
Custom agents	**Sculptor.** Turns a described playbook into a governed agent.	**Agent Builder.** Natural-language agent creation with reusable skills.

Custom Agents: Sculptor and Agent Builder

ASPECT	SELECTOR SCULPTOR	CISCO AGENT BUILDER
Definition	A playbook in plain language becomes an agent with goal, context, approved tools, and limits.	Agents described in natural language; runbooks and SOPs become reusable skills.
Triggers	Chat, event, schedule, API call, or another agent.	Ambient agents run continuously; live agents are invoked in AI Canvas sessions.
Lifecycle	Build, test, version, and govern agents on the customer's own data.	Draft, sandbox, and publish; versioned and immutable with rollback.
Control points	Required human approval points per agent; acts on high-confidence findings.	Customer defines what agents can do and when; humans approve before production changes.
Audit	Every run recorded with trigger, evidence, actions, and outcome.	Splunk AI Agent Monitoring traces every execution.
Acts on	Deterministic, multi-vendor root cause findings.	Cisco Cloud Control context and connected tools.

Cisco Cloud Control gaps

- Agents reason over Cisco context; non-Cisco data reaches them only through connectors.
- No incident communications agent described; ITSM runs through connectors.
- Agent Builder was announced in June 2026, on a platform in U.S. Controlled Availability.

Selector value

- Six specialized agents covering investigation, RCA, ITSM, views, communications, and custom agents.
- Agents act only on deterministic, multivendor root cause findings.
- Sculptor agents run from chat, events, schedules, APIs, or other agents, with approval points and audit.

Copyright Selector Software, Inc.

Agent Integration and Governance

ASPECT	SELECTOR MCP SERVER	CISCO CLOUD CONTROL
Role	Selector acts as an MCP server, exposing topology, dependencies, and correlated telemetry to external agents.	Cloud Control consumes first- and third-party tools through MCP and A2A gateway patterns.
Access control	Single endpoint secured with OAuth2; granular RBAC over insights, recommendations, and actions.	Inline RBAC translation layer across product permission models; least privilege by design.
Runtime	Dedicated Kubernetes node isolated from core services; elastic scaling; self-healing.	Cisco AI Defense intercepts LLM calls and tool invocations to block unauthorized use and prompt injection.
Audit	Every interaction between agents, Selector, and connected systems is auditable.	Full auditability; Splunk AI Agent Monitoring traces tool use.
Extensibility	Works with standard agent frameworks without custom adapters; A2A supported.	**Customer and partner built MCP connectors planned, not available.**

Deployment

LAYER	SELECTOR	CISCO CLOUD CONTROL
Deployment model	SaaS, on premises, customer cloud, or air gapped.	Cloud-delivered. **On premises and air gapped options not described.**
Platform	Kubernetes-native; collection engines near data sources, outbound-only.	Federated architecture with micro front ends and shared platform services.
Delivery	Full platform and every Foundry agent available now.	U.S. Controlled Availability since June 2026; features when-and-if available.

Cisco Cloud Control gaps

- Cloud-delivered only; on-premises and air-gapped options not described.
- Customer and partner built MCP connectors are planned, not available.
- U.S. Controlled Availability; features offered when-and-if available.

Selector value

- Production MCP server with OAuth2, granular RBAC, isolated runtime, and full audit.
- SaaS, on-premises, customer cloud, or air-gapped deployment.
- Full platform and every Foundry agent available now.

Copyright Selector Software, Inc.

Delivered with Forward Deployed Engineers

Selector is delivered as a platform plus forward deployed engineers who partner with each customer to build the outcomes its operation needs: integrations, data models, operational views, and governed agents built to its requirements. Cisco Cloud Control provides self-service tools for customers and partners to build their own.

OUTCOME	SELECTOR, BUILT WITH FORWARD DEPLOYED ENGINEERS	CISCO CLOUD CONTROL
Integrations	Engineers normalize supported API, CMDB, database, and file sources into one operational model. MCP exposes findings to external agents; A2A enables agent interoperability.	Native connectors through Cloud Control Studio (50+ planned); customers build MCP connectors once available, or use SDKs.
Data model and logic	Engineers encode the customer's enrichment, labels, noise rules, maintenance windows, and criticality in YAML and S2ML.	Customer builders upload runbooks and SOPs as agent skills. **Customer defined enrichment, labels, and noise rules not described.**
Operational views	Engineers build topology views, drill-downs, and dashboards from the customer's CMDB and network design data, backed by query chains.	AI Canvas generates cards per investigation; customers and partners build apps with SDKs and contribution contracts.
Agents and workflows	Engineers convert the customer's runbooks into governed Sculptor agents connected to ITSM and collaboration tools.	Self-service Agent Builder; partner-built agents in a Marketplace Cisco expects to mature over the next two to three years.
Delivery model	Selector engineers work alongside the operations team on a weekly delivery cadence.	Self-service build tools, headless modes, CLIs, and AI-assisted development. **Cisco engineered, customer specific outcomes not described.**

How the Engagement Works

1. Capture requirements

Engineers work with the operations team to define the views, integrations, and workflows the team needs.

2. Build on your data

Outcomes are built from the customer's own CMDB, inventory, telemetry, and network design data.

3. Review weekly

Results are reviewed with the team each week, and requested changes are delivered in the following sprint.

4. Operationalize

Completed outcomes become governed platform capability, not one-off scripts the team must maintain.

Cisco Cloud Control gaps

- The build model is self-service: customer engineers write apps and agents with SDKs, CLIs, and AI-assisted development.
- Cisco does not describe its own engineers building customer-specific views, integrations, or agents.
- Third-party connectors and customer-built MCP connectors are planned, not available.

Selector value

- Engineers partner with the team to build outcomes to its requirements, on its own data.
- Custom views, integrations, and agents become governed platform capability.
- Requested changes are delivered on a weekly cadence.

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

Selector vs. Cisco Cloud Control at a Glance

The layer-by-layer differences translate into the following value compared with Cisco Cloud Control.

VALUE	SELECTOR	CISCO CLOUD CONTROL
Full-Estate Data	One normalized model across every vendor, cloud, and system of record.	Cisco portfolio; cloud through Multicloud Defense (security) and Multicloud Fabric (beta); other tools through connectors.
Raw-Signal Correlation	Raw telemetry and context correlated at ingestion, before an incident opens.	Third-party tools connected for context and actions.
Causal Root Cause	Causation models over topology and domain logic; LLM-agnostic; every finding traceable.	LLM reasoning over converged Cisco context.
Reproducibility	Raw data retained with original timestamps; Network DVR replay.	AI Canvas investigation record and agent traces. **Network state replay not described.**
Prediction	Optical failure prediction and capacity forecasting.	**Not described in Cloud Control materials**.
Your Playbooks as Agents	Sculptor builds governed agents that act on verified findings.	Agent Builder converts runbooks into agent skills.
Delivered Today	Full platform and every Foundry agent available now.	U.S. Controlled Availability; features when-and-if available.
Coexistence	Ingests Cisco and non-Cisco telemetry alongside existing tools; shares operational context and root-cause findings with compatible agents through MCP.	Complements existing Cisco controllers; incorporates third party data and actions through supported integrations and MCP

The Bottom Line

Cisco Cloud Control is a cross-product control plane that converges Cisco domain products under shared identity, inventory, topology, and policy, with AI Canvas and Cloud Control Studio built on top.

Selector is a data-centric intelligence layer. It collects raw telemetry and context from every vendor, preserves and enriches it before analysis, establishes deterministic causation with purpose-built models, and puts governed agents on top, including agents Sculptor builds from your own playbooks. It is available now in every deployment model, including on-premises and air-gapped, and it works alongside Cisco tooling.

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.