E3 CreaTIC

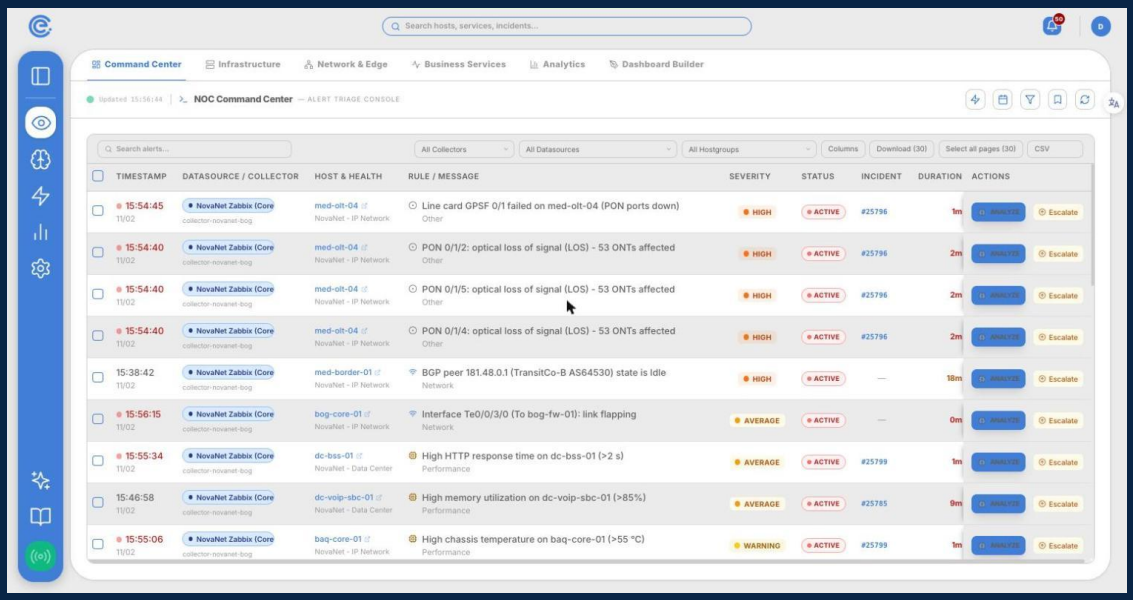
DATASHEET · 2026

AIOPS & OBSERVABILITY PLATFORM

EVA AIOps

Intelligent Operations & Proactive Support

Connect every monitoring and telemetry source, turn thousands of alerts into a few incidents with their probable cause, and orchestrate the response.



Multi-source collection · **Correlation** · **Anomalies** · **Root cause** · **Generative AI** · **Orchestration**

From alert noise to actionable incidents

Reduce MTTR by operating with less noise, more accurate diagnoses and concrete notification and/or resolution actions.

The operations challenge

Operations and technology service support centers deal with thousands of alerts a day, spread across several monitoring tools, logs, traps and network flows. Most of them are repeated symptoms of the same problem, and the team loses valuable time deciding what to look at first while the service is already degraded.

Monitoring tools know **that something failed**; the hard part is understanding **what failed first, who is affected and what to do now**. That answer usually depends on the experience of whoever is on shift, and it results in longer than necessary detection (MTTD) and resolution (MTTR) times.

At a glance

EVA AIOps is the intelligence layer between your monitoring and your team. It collects data with **EVA Collector** (SNMP, Syslog, NetFlow, OpenTelemetry, agents, APIs) or connects to the platforms you already own: **Zabbix, PRTG, SolarWinds, Prometheus/Grafana, Elastic, Splunk** and other sources.

It normalizes events and enriches them with the CMDB, groups them into incidents, detects anomalies, ranks root-cause candidates with visible evidence, calculates business impact and triggers workflows that notify, open tickets and run remediation actions without writing code.

One platform, four layers

EVA AIOps covers the full operations cycle: from raw data to action.

01
Data Collection & Integration

Collects information from multiple sources, platforms and technologies through connectors and native infrastructure.

- EVA Collector
- Monitoring platform connectors

02
Intelligent Event Processing

Normalization, deduplication, correlation, enrichment and intelligent event analysis with AI/ML algorithms.

03
AIOps & Observability

Incident identification, anomaly detection, pattern analysis, identification of probable root causes and operational visibility.

04
Automation & Orchestration

Integration with ITSM platforms, notifications, ticket generation, action execution and auto-remediation processes.

Proven results

69%
alert noise reduction

56%
improvement in incident response

36%
MTTR improvement in the first year of implementation

100k+
assets managed

Figures from EVA deployments at telecommunications customers, validated by success story; the launch pilot achieved a 97.9% noise reduction. Results depend on each customer's operational volume and infrastructure.

Operational outcomes

Less noise

Duplicate and related alerts are grouped into a single prioritized incident. The noise-reduction indicator measures it continuously.

Lower MTTR

Early detection through anomalies, probable cause in seconds and automated response: less time between alert and fix.

Explainable diagnosis

Every root cause shows the evidence behind it. Operators understand why, not just what.

Business view

For every business service you model in EVA: its health, potentially affected users, revenue at risk per hour and SLA compliance.

EVA Collector: multi-protocol collection

EVA Collector is EVA's collection and normalization component. It is deployed on the customer network (data center, branch sites or cloud) and captures telemetry from any source using the mechanism that best fits each component, with no dependency on a third-party monitoring tool.

Mechanism	Standards and protocols	Coverage
Agent-based	EVA Collector OS-level agent with eBPF (extended Berkeley Packet Filter, a Linux kernel technology for low-overhead system observability) or equivalent technology	Physical and virtual servers and container nodes: metrics, logs, events and traces
Agentless	SNMP v1/v2c/v3 (polling and traps), SSH, WMI and Syslog (RFC 3164 / 5424)	Network and security devices, storage, printers, UPS units, precision air conditioning and any other SNMP device, legacy environments and log-producing platforms
Network flows	NetFlow, sFlow and IPFIX	Traffic, bandwidth and conversations on network links
Open standards	OpenTelemetry (OTLP) and Prometheus / OpenMetrics exporters	Instrumented applications, containers, Kubernetes clusters and databases
APIs and files	Cloud and vendor REST APIs, inbound webhooks and log files	Public clouds (Azure, OCI, AWS), vendor consoles and in-house applications

DEPLOYMENT

Ready in minutes

- Docker container with an install command generated by the console
- Outbound encrypted connections only (HTTPS 443): no inbound ports opened on your network
- Centrally managed configuration

RESILIENCE

No data loss

- Persistent local buffer of up to 100,000 events during outages
- Delta-only transmission
- Fallback URLs

SECURITY

Protected at the source

- Enrollment secret, administrator approval and renewable token
- TLS 1.2/1.3 and mTLS; optional IPsec VPN
- Revocation and hardware identity

Integration with the monitoring platforms you already own

If your organization has already invested in one or more monitoring platforms, EVA **does not replace them: it unifies them and adds intelligence**. Its connectors consume alerts, events, metrics and inventory from each tool and process them into a single incident model, so the team works from one console and one source of truth.

Platform	Data EVA consumes	Integration method
Zabbix	Problems and alerts, metrics and history, inventory and host groups, proxies for remote diagnostics	Native API

Platform	Data EVA consumes	Integration method
PRTG Network Monitor	Sensor alarms and states, devices and groups, channel values	API and webhook notifications
SolarWinds	Active alerts, nodes, interfaces and element status	API (SWIS) and webhook
Prometheus / Grafana	Alertmanager and Grafana alerts, metric series	Webhook receiver and query API
Elastic	Rule alerts, logs and events	API and webhook connector
Splunk	Scheduled-search alerts and notable events	Webhook alert action and REST API
Other sources	Nagios, Icinga and any system that emits Syslog, SNMP traps or webhooks, or exposes a REST API	EVA Collector and generic connectors

How EVA lowers MTTR on top of your current monitoring

DETECT
Earlier, with less noise
Anomalies against each metric's baseline and alerts from every source correlated into one incident.

DIAGNOSE
Probable cause in seconds
Root-cause candidates with evidence, topology, similar incidents and an AI-generated summary.

ESCALATE
To the right team
Priority based on the affected service; automatic ticket and notification with full context.

RESOLVE
With one click, or none
Remote diagnostics and remediation workflows; auto-close when no active alerts remain.

LAYER 2 · INTELLIGENT EVENT PROCESSING

From raw event to incident

Every event is normalized, enriched with context and correlated with the others so that only real incidents reach the team. Grouping decisions are made with auditable rules and evidence.

Normalization and enrichment

- **Common event model** for every source: harmonized severity, device, service, category and environment.
- **Automatic classification** by keywords and environment (production, staging, development) plus an override table by name pattern.
- **CMDB context**: owner, contract, SLA, supported services and impacted customers from InvGate Asset Management or any CMDB via API.
- **Historical data**: baselines, recurrence and similar incidents from the last 90 days.

Deduplication, correlation and noise reduction

1 incident, not 50 alerts. The staged correlation engine turns thousands of alerts into a few actionable incidents.

- **Deduplication** of repeated alerts and association of new alerts with the open incident of the same device.

- **Custom rules** with priority, scope, conditions, time window and title template; **pattern extractors (regular expressions)** to group by location, device, server or application name, BGP peer, PON port, OLT or any other key.
- **Multi-dimensional AI/ML grouping**: device, topological neighborhood, message similarity, time proximity, category and environment.
- **Noise-reduction indicator**: raw alerts versus generated incidents, per rule and per stage.

LAYER 3 · AIOPS & OBSERVABILITY

Explainable AIOps intelligence

Each engine answers a different operational question and delivers its result with the reasoning behind it, so operators can decide with confidence. Generative AI explains and accelerates; it never decides without evidence.

Incident identification and management

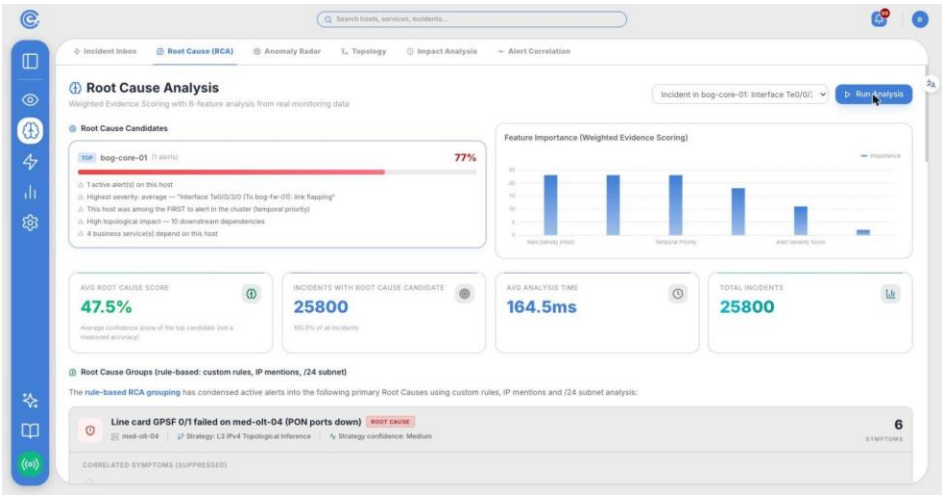
- Prioritized incidents (P1 to P3) with a full lifecycle: assignment, individual or bulk acknowledgment, notes, timeline and auto-close when no active alerts remain.
- Advanced search over incident, CMDB and correlation fields; saved views shared across the team.

Anomaly radar

- Multi-layer architecture: **Z-Score and interquartile range (IQR)** against each metric's baseline, **adaptive trend (exponential moving average)** and **generative AI explanations**.
- CPU, memory, disk, swap, load, interface traffic, latency and packet loss, among others.
- Detects degradation before a fixed threshold is crossed; auto-resolves on normalization and can trigger automations.

Root cause with weighted evidence scoring

- Prioritized list of candidates with six weighted pieces of evidence: **severity, alert density, topological depth, temporal priority, service criticality and symptom diversity**, with each one's contribution shown.
- Symptom grouping by rules, mentioned IPs and subnet; root-cause tree, similar incidents and a 7×24 recurrence heat map.



Root cause analysis: top candidate and its weighted evidence

Topology and business impact

- Dependency graph with relationships declared in the CMDB and inferred ones (co-occurrence, incident chains, subnet, services).
- Blast radius, impacted services, estimated users, **revenue at risk per hour** and propagation chain from the root cause.

Generative AI for operations

- **Conversational assistant** that queries live data from your environment and an **AI narrator** that produces an executive summary of the current view.
- **Incident summary** with probable causes and suggested solutions; alert analysis and anomaly explanations in natural language.
- Model-agnostic: **local with Ollama** or any OpenAI-compatible API, with the customer in control of its data.

Application observability and digital experience

Extends EVA's visibility from the infrastructure to the application and the end user, with the same correlation, anomaly and root-cause engines.

Capability	Scope
Application performance monitoring (APM)	Distributed tracing with OpenTelemetry (auto-instrumentation for Java, .NET, Node.js, Python and Go); service map; request rate, errors and duration per service and transaction; trace explorer; correlation between traces, logs and infrastructure metrics.
Real user monitoring (RUM)	Lightweight component for web applications that measures page load, Core Web Vitals, JavaScript errors and service calls by browser, device and location, and links them to server-side traces.
Synthetic monitoring	Scheduled tests from EVA Collectors at different sites: HTTP/HTTPS (status code, content and certificate expiry), DNS, TCP, ICMP, multi-step APIs and recorded browser transactions; availability and response time against SLA.

Visibility for every role

View	What it answers
Command center	Real-time console for the operations and service support center: every alert from every source, filters, per-resource health, AI analysis and escalation to incident.
Incident inbox	Correlated, prioritized incidents with their probable cause, CMDB context and history.
Infrastructure and network	Server and network device health: indicators, top consumers, per-interface traffic, latency and loss.
Business services	Health of each business service, components, MTTR, SLA and the incidents affecting it.
Analytics and reports	Trends, noisiest components, MTTR/MTBF, availability vs. SLA, noise reduction; export to PDF, CSV and JSON.
Event explorer	Search of Syslog, SNMP traps, flows and webhooks received by the collectors, with CMDB context and original content.

View	What it answers
Dashboard builder	Custom dashboards with real-time indicators, charts, gauges and tables.

LAYER 4 · AUTOMATION & ORCHESTRATION

From diagnosis to action

Visual **no-code** workflow designer on a durable execution engine, with per-step retries and compensation steps.

- **Triggers**: alert, incident and anomaly events with conditions; signed inbound webhook (HMAC) and periodic scheduling.
- **Automatic or manual mode**: each rule runs its workflow in the background or publishes an action button in the console.
- **Actions**: escalate, prioritize, acknowledge, comment and resolve incidents; remote diagnostics (ping, traceroute, ports, DNS, HTTP) and auto-remediation actions.
- **Logic**: conditions, fork and join, loops, waits and data parsing. Execution history with step-by-step detail.

Type	Connectors
Notification	Microsoft Teams, Telegram, Slack and email (SMTP)
ITSM	Create, comment, update and query tickets in any ITSM with a REST API
CMDB	InvGate Asset Management and other CMDBs via API
Generic	Web service (Bearer, basic, API key, OAuth2) and outbound webhook

Use cases

TELECOMMUNICATIONS & ISPS

Network and access operations

Correlation of OLT, BNG, BGP and backbone failures; impact on subscribers and residential services.

ENTERPRISE IT

IT operations

One console across multiple monitoring tools, with CMDB, SLA and automatic ticketing.

MANAGED SERVICES

Multi-customer operations

Dedicated instances per customer, remote collectors and SLA and performance reports.

Technical specifications

Monitoring sources	Zabbix, PRTG, SolarWinds, Prometheus/Grafana, Elastic and Splunk; other sources via Syslog, SNMP traps, webhooks and REST API.
EVA Collector	Agent (eBPF or equivalent); agentless: SNMP v1/v2c/v3, SSH, WMI, Syslog; NetFlow, sFlow, IPFIX; OpenTelemetry (OTLP), Prometheus/OpenMetrics; cloud (Azure, OCI, AWS) and vendor APIs; log files.

Collector deployment	Docker container on the customer network; outbound HTTPS (443) connections only; enrollment secret, approval and renewable token; persistent buffer of up to 100,000 events; fallback URLs.
Processing and AIOps	Staged correlation (rules, regular expressions, AI/ML), anomaly radar (Z-Score, IQR, exponential moving average), root cause by weighted evidence scoring, topology and business impact.
Generative AI	Ollama (local) or any OpenAI-compatible API; configurable parameters and instructions.
Outbound integrations	Teams, Telegram, Slack, SMTP, InvGate Service Desk and Asset Management, generic web service and webhook.
Security and access	Role-based access control with system and custom roles (resource:action); bcrypt passwords and JWT sessions; exportable audit log; TLS 1.2/1.3, mTLS with collectors, HSTS and masked secrets.
Deployment model	Dedicated instance per customer with isolated data: dedicated SaaS on AWS or on the customer's infrastructure.
Applications and digital experience	APM with OpenTelemetry traces, real user monitoring (RUM) and synthetic monitoring from the collectors.
Platform	Python services (FastAPI), PostgreSQL, Redis, Kafka, OpenSearch, Neo4j, MinIO and Temporal; React web UI with per-user time zone.

Getting started

01
Connect
Register your monitoring platforms and install EVA Collector on your network.

02
Tune
Model your business services, connect the CMDB and define correlation rules.

03
Automate
Design response workflows: tickets, notifications and remediation.

About E3 CreaTIC

E3 CreaTIC is a Colombian company, founded in 2012, that develops software and integrates AIOps, observability, monitoring, ITSM and ITAM solutions for network and IT operations. We have delivered projects in more than 16 Latin American countries and more than 200 automations and integrations. We are a Zabbix Delivery Partner and an InvGate Gold Partner. **EVA AIOps is our product: we design it, build it and support it.**

Web e3creatic.com · **Email** sales.latam@e3creatic.com · **Phone** +57 324 399 3791

Office Av. El Dorado #92-32, Of. 5-131 · Bogotá, Colombia

Live demo demo-eva.e3creatic.com · **User manual** e3creatic.com/es/productos/eva-aiops/docs · **Support** support.e3creatic.com

© 2026 E3 CreaTIC. All rights reserved. EVA AIOps is a product of E3 CreaTIC. Zabbix, PRTG, SolarWinds, Nagios, Icinga, Prometheus, Grafana, Elastic, Splunk, InvGate, Microsoft Teams, Telegram, Slack, OpenAI, Ollama and the other brands mentioned belong to their respective owners and are cited for identification purposes only. The capabilities described may change without notice.