NIRVET

NETWORK INTELLIGENCE · RISK VISIBILITY · EVENT TRIAGE

Technical Overview

Detection, investigation, and response at machine speed — with human control.

Nirvet consolidates detection, investigation, and response across hybrid environments into a single, governed plane. AI co-pilots accelerate every step of the analyst workflow, while an explicit authority model ensures automation moves fast without moving recklessly. This overview summarises the platform's architecture, capabilities, security posture, and deployment options.

Deployment	SaaS, private cloud, on-premises, air-gapped, hybrid
Tenancy	Multi-tenant with per-tenant data isolation (row-level security)
Response coverage	Microsoft (Defender / Entra / M365), Okta, CrowdStrike — expanding
Governance	Authority-to-act ladder · four-eyes approval · reversible actions
Compliance	Built to support NIS2, DORA, HIPAA, ISO 27001, PCI-DSS

1 · Executive Summary

Security teams face more alerts than they can triage, context scattered across many consoles, and mounting pressure to contain incidents fast. Nirvet addresses this by unifying telemetry, using AI to correlate and summarise, and governing every response action through an authority model an auditor would recognise as sound — the speed of automation with the accountability of human oversight.

- One plane for detection, investigation, and response across EDR, SIEM, cloud, identity, and network telemetry.
- AI-assisted triage and investigation summaries that reduce analyst cognitive load.
- Governed, reversible response actions across leading security vendors.
- Built for both in-house SOCs and managed security service providers (MSSPs).

2 · Platform Architecture

Nirvet is organised as a pipeline: ingest !’ normalise !’ detect !’ correlate !’ investigate !’ respond, with evidence capture and audit spanning the whole flow. Telemetry from many sources is normalised to a canonical schema so detection content and investigations work uniformly across vendors. Every tenant's data is isolated at the database layer using enforced PostgreSQL row-level security, so one customer can never read another's data.

- Canonical event schema — vendor telemetry mapped to one model for consistent detection and search.
- Per-tenant isolation via forced row-level security; multi-tenant by design for operators.
- Deployment models: SaaS cloud, private cloud / on-prem, air-gapped, and hybrid / federated collection.
- Cloud-portable storage and evidence layers; region-aware endpoints including sovereign / GovCloud.

3 · Detection & Correlation

Detection is pluggable and content-driven. Analysts author rules in familiar languages, and stateful primitives express behaviour over time — not just single-event matches. Correlated signals are scored to produce a ranked queue of decisions rather than a flood of raw alerts.

- Pluggable detection DSLs (Sigma and CEL) with a curated starter content library.
- Stateful primitives — count, window, and sequence — for behaviour-based detection.
- Alert correlation and risk scoring that group related signals into high-confidence findings.
- MITRE ATT&CK technique mapping and coverage analytics.

4 · Response & Automation (SOAR)

Response is where Nirvet's governance is most visible. Playbooks are versioned and auditable; steps enrich, collect evidence, notify, and execute real vendor actions. Every action is gated by an authority policy, and the highest-consequence actions require human approval — with a defined, safe way to undo them.

> **Authority-to-act ladder** — Each action type is governed by a mode: observe, approval-required, pre-authorized, or contractual-auto. Business-critical assets never auto-run under any mode, and configuration can only tighten a stricter global default, never loosen it.

> **Fleet-wide guardrail** — Actions with tenant-wide blast radius (e.g. a tenant-wide IOC block) are always approval-first and human-run, independent of how reversible they are — breadth is treated as its own risk axis.

- Four-eyes approval gates on high-consequence actions; break-glass and per-action timeout policies.
- Reversible by design — actions carry a defined inverse, and a reversal only ever undoes what the run actually changed.
- Vendor actioners: Microsoft Defender host isolation, Entra account disable, M365 controls; Okta session/account; CrowdStrike host containment and fleet-wide IOC block.
- No hardcoded thresholds — authority, timeout, and break-glass are admin-configurable policy records with safe seeded defaults.

5 · AI Co-pilot & Governance

The AI co-pilot accelerates triage and investigation — summarising timelines, surfacing entities, and proposing next steps and response actions — while a human always makes the decision. Critically, AI runs behind a governance layer so sensitive data is handled on the customer's terms.

- Egress redaction fence with a zero-config floor: an empty policy means redact everything, never send everything.
- Admin-controlled LLM provider and explicit per-tenant model allowlist — governance is configuration, not code.
- Versioned prompt registry with a hermetic evaluation harness and a CI fence — prompt changes are tested, not shipped blind.
- Human-in-the-loop by default; per-tenant isolation, customer-approval, and retention controls carry into every AI interaction. No training on customer data.

6 · Evidence & Chain of Custody

Investigations are only as defensible as their evidence. Every artifact is hashed on capture, timestamped, and stored with provenance, preserving chain of custody from collection through export.

- Cryptographic hashing on capture; integrity verifiable at any later point.
- Full custody trail — who collected what, when, from where, and every hand-off since.
- Legal hold that overrides routine retention; retention-delete that is atomic and auditable.
- Signed, self-describing evidence packages for regulators, auditors, or counsel.

7 · Integrations & Connectors

Nirvet meets your stack where it lives. A guided connector wizard onboards each source (create !' configure !' test); ingestion mappers normalise telemetry; and response actioners reach back into your tools. All outbound calls run through an SSRF-safe egress layer, and credentials are encrypted at rest.

- Source connectors across EDR, SIEM, cloud, identity, and email, with per-tenant configuration and health visibility.
- Outbound ticketing (ServiceNow, Jira) and multi-channel notifications (email, SMS, chat).
- Response actioners expanding across identity, endpoint, and network vendors.
- SSRF-guarded egress, encrypted credentials, and authority-gated, audited connector actions.

8 · Security, Trust & Compliance

Nirvet holds itself to the standard it helps customers enforce. Security is built in, not bolted on.

- Encryption in transit (TLS 1.3) and at rest (AES-256); customer-managed keys (BYOK / HSM) for enterprise tenants.
- Zero-trust access — every API call and UI action authorised against policy, with a full, exportable audit trail.
- Session security: httpOnly cookie sessions, CSRF protection, rotating refresh, and platform-wide session revocation.
- SSO via SAML 2.0 / OIDC, SCIM provisioning, and enforced multi-factor authentication.
- Built to support NIS2, DORA, HIPAA, ISO 27001, and PCI-DSS; responsible vulnerability disclosure and annual third-party penetration testing.

9 · Deployment & Operations

Nirvet is designed to meet your data-residency posture, and to be operated with confidence at scale.

- SaaS, private cloud / on-prem, air-gapped, and hybrid deployment — full data-residency control where required.
- Observability: Prometheus metrics, health / readiness endpoints, and distributed tracing (OpenTelemetry).
- Operational safety: schema-validated migrations, CI guards, rate limiting, and graceful degradation modes.
- Multi-tenant operations for MSSPs — granular RBAC, per-tenant isolation, and consolidated management.

10 · Engagement Models

Operate Nirvet yourself, or have our team run the SOC function on your behalf. Both models share the same governance, isolation, and evidence guarantees.

- Nirvet Platform (self-operated) — your team, your environment, full control of data and playbooks.
- Nirvet MSSP (fully managed) — dedicated analyst coverage, proactive threat hunting, and defined response SLAs.

11 · Talk to Us

This overview is a summary; we're happy to go deeper on any area, share architecture detail, or scope a proof of concept.

- General enquiries: contact@nirvet.com
- Sales & demos: sales@nirvet.com
- Security & disclosure: security@nirvet.com