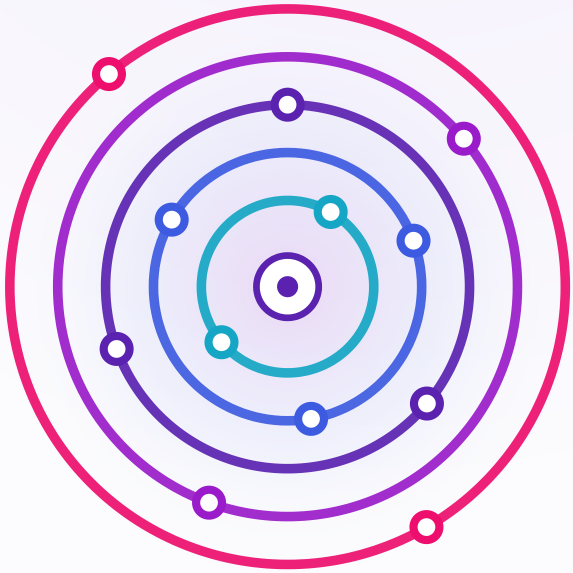
TRIQUETRA

VISIBILITY · INTELLIGENCE · AUTOMATION

AI-POWERED SECURITY PLATFORM

SOLUTION WHITE PAPER

Converge360™



Five layers. Twelve components. One platform.

Triquetra Converge360™ is an AI-powered security singularity platform that converges visibility, intelligence and automation — threaded end to end by an agentic AI fabric, beneath a single source of truth.

- L1 INGESTION
- L2 FOUNDATION
- L3 INTELLIGENCE
- L4 OPERATIONS
- L5 EXPERIENCE

01 EXECUTIVE SUMMARY

Security has outgrown the multi-tool era.

Cybersecurity is no longer a back-office concern — it is a board-level question of business survival. Yet the way most enterprises defend themselves has quietly become the problem itself.

As organisations scale, they accumulate point tools — SIEM, EDR, DLP, IAM, CSPM, GRC and dozens more — each with its own console, its own data model, and its own blind spots. The intent is defence in depth. The reality is **defence in fragments**: analysts switching between a dozen dashboards, correlating incidents by hand, and still missing the one signal that mattered. More tools have not produced more security; they have produced more noise, more silos, and more places for a threat to hide.

Triquetra Converge360™ exists to end that fragmentation. It is an **AI-powered, SOAR-integrated, compliance-ready singularity platform** that unifies visibility, intelligence and automation into a single source of truth. Rather than bolting consoles together, Converge360 is built as **five cooperating layers and twelve components** beneath one dashboard — ingestion, foundation, intelligence, operations and experience — and threaded throughout by an **agentic AI fabric** that reasons alongside the platform at every stage. Raw signal enters at the edge; coordinated, accountable action comes out the top.

This white paper sets out the problem that unified platforms solve, the industry forces driving consolidation, and the layered architecture that lets Converge360 deliver a genuine 360° view — turning chaos into coordination, silos into synergy, and alerts into action.

- **5 layers · 12 components**
- **300+ native integrations**
- **Agentic AI / LLM fabric**
- **Compliance-ready by design**
- **SOAR-integrated automation**

02 THE CHALLENGE

Fragmented security environments.

A typical enterprise runs SIEM, EDR, DLP, IAM, CSPM and more — each with its own dashboard. The result is fragmented visibility and siloed data, and it shows up as four recurring failures.

Alert fatigue

Teams are buried under alerts from every system — a large share false positives or duplicates. Critical incidents slip through simply because no one can sift the volume in time.

IN PRACTICE

A global enterprise running separate SIEM and EDR consoles missed a ransomware attack in the noise, leading to significant data loss.

Manual workflows

Without integrated automation, response is slow, manual and error-prone. Analysts spend hours correlating data by hand — time that containment and mitigation simply don't have.

IN PRACTICE

A financial firm's disparate detection tools forced manual handling; an attack containable in minutes took hours to resolve.

Data silos

When security data lives in unconnected systems, teams cannot correlate or contextualise incidents. The gaps between tools become the gaps in defence.

IN PRACTICE

An IT provider couldn't link phishing alerts from its email gateway to endpoint anomalies — leaving the threat picture incomplete.

Compliance complexity

Audit readiness suffers when evidence is scattered across tools. Consolidating trails and producing reports becomes a cycle of manual effort — and a standing risk of non-compliance.

IN PRACTICE

A healthcare provider was fined after failing to consolidate IAM and DLP audit logs, leaving gaps in data-integrity verification.

03 INDUSTRY TRENDS & STATISTICS

The market is consolidating — fast.

Security leaders are converging on a single conclusion: the fragmented, multi-vendor model has reached its limit. The evidence is consistent across the major analysts.

70%

of CISOs prioritise unified security dashboards

Consolidating IAM, SIEM, DLP, EDR, CSPM and GRC into one source of truth to reduce risk exposure.

GARTNER, 2025

50%

faster incident response with integrated management

Unified data enables faster correlation and actionable insight, cutting time-to-respond in half.

FORRESTER, 2025

80%

of leaders cite fragmented dashboards as a key barrier

Fragmentation hampers visibility and creates operational drag on effective threat response.

CYBERSECURITY VENTURES, 2024

45%

growth in SOAR adoption over two years

Automating response and correlation cuts manual workload and human error, driving demand for SOAR-enabled platforms.

IDC, 2024

The pattern is unambiguous. Legacy, multi-vendor ecosystems impose a measurable tax — in dwell time, in analyst hours, and in audit risk — and the organisations removing that tax are the ones consolidating onto unified, automated, AI-assisted platforms. Downstream, the same studies show **AI-driven detection improving accuracy by ~30%** (Gartner, 2024), **SOAR cutting resolution times by ~60%** (Forrester, 2025), and **centralised compliance reducing audit-prep effort by ~40%** (Ponemon Institute, 2024). The question is no longer whether to converge, but onto what.

04 THE CASE FOR CONVERGENCE

Why enterprises need a unified platform.

A unified platform is not a cosmetic merge of dashboards — it changes what a security team can see, how fast it can act, and how confidently it can prove control.

Real-time visibility

One view consolidates every tool into a 360° picture of the risk landscape.

- No tab-switching — analysts act on critical alerts immediately
- Contextual correlation across SIEM, EDR and IAM in one place
- Executive-level risk metrics without interpreting raw feeds

Efficient threat detection & response

Built-in SOAR automates response, cutting manual effort and human error.

- Automated playbooks for consistent, swift reactions
- Predictive, AI-driven anticipation of emerging vulnerabilities

–60% incident resolution time with SOAR (Forrester, 2025)

Streamlined compliance & reporting

Automated aggregation across ISO, GDPR, NIST, SOC 2 and HIPAA.

- Audit-ready documentation generated consistently
- Real-time checks surface compliance gaps before audits

–40% audit-preparation time (Ponemon Institute, 2024)

AI-driven decision-making

AI and LLMs turn raw data into foresight and plain-language insight.

- Contextual recommendations from historical and live data
- Risk forecasting that suggests mitigation early

+30% threat-detection accuracy (Gartner, 2024)

05 THE CONVERGE360 ARCHITECTURE

Five layers. One platform.

Converge360 is not a bundle of consoles — it is a single pipeline built as **five cooperating layers and twelve components**. Each component does one job well and hands clean output to the layer above, so signal enters at the edge and emerges at the top as coordinated action. An **agentic AI / LLM fabric** threads through every layer, reasoning alongside the platform end to end rather than being bolted on as a feature.

L5 Experience
The single pane of glass — dynamic dashboards, reports, forms and a mobile app for the whole team.

`11 Dashboard` `12 Mobile App`

L4 Operations
Turns verdicts into coordinated action — workflow automation, task ownership and multi-channel notification.

`08 Workflow` `09 Task Management` `10 Notification`

L3 Intelligence
Turns entities into judgment — rule logic, threat intelligence and correlation into timeline-ordered incidents.

`05 Rule Engine` `06 Threat Intelligence` `07 Correlation Engine`

L2 Foundation
Resolves raw signal into canonical truth — one trusted record for every identity and asset (the who and the what).

`03 Identity Fabric` `04 Asset Registry`

L1 Ingestion & Discovery
The boundary — vendor-agnostic connectors bring the known in; active scanning uncovers the unknown.

`01 EdgeBridge` `02 Discovery Tools`

AGENTIC AI / LLM FABRIC

Reasons alongside every layer — enriching, correlating, drafting and recommending end to end.

↑ RAW SIGNAL IN AT L1 · COORDINATED ACTION OUT AT L5 · DATA FLOWS UPWARD ↑

The effect is compounding. Because every layer inherits clean, trustworthy input from the one below, judgments are made on canonical entities rather than raw logs, action is driven by correlated incidents rather than isolated alerts, and the dashboard reflects exactly what the platform knows. Each layer is documented in its own detailed datasheet — L1 Ingestion & Discovery, L2 Foundation, L3 Intelligence, L4 Operations and L5 Experience.

Detailed per-layer datasheets (L1–L5) are available as companions to this white paper.

06 THE SOLUTION

How Converge360 addresses these challenges.

Five platform capabilities map directly onto the four failures of fragmentation — each turning a chronic weakness into an operational strength.

1 Unified security visibility

SINGULARITY SECURITY DASHBOARD · L1 + L5

Agent-less, real-time visibility across on-premises, cloud, hybrid and remote — aggregating IAM, SIEM, DLP, EDR, CSPM, GRC and third-party APIs into one Security Graph, with XDR-ready architecture and external attack-surface monitoring.

OUTCOME No tab-switching, blind spots or context gaps — one 360° live view of your posture.

2 AI-driven threat intelligence & posture management

AI-SPM ENGINE · L3

Predictive analytics, behavioural baselining and LLM-powered enrichment turn raw logs into plain-language insight, flag anomalies across users, access, network and cloud, and visualise attack paths to block lateral movement before it spreads.

OUTCOME Earlier detection of stealthy, multi-stage attacks through contextual threat modelling.

3 SOAR integration & adaptive automation

VISUAL PLAYBOOK BUILDER · L4

Native integration with 300+ security tools, event-driven no-code/low-code workflows (or Python), and playbooks with trust-level scoring and escalation logic that optimise time-to-detect and time-to-contain.

OUTCOME From triage to containment, every step automated — without sacrificing control.

4 Compliance, trust & audit-ready assurance

TRUST MANAGEMENT FRAMEWORK · CROSS-CUTTING

Policy-aware automation aligned to ISO 27001, GDPR, NIST 800-53, SOC 2, HIPAA and MAS TRM / RMiT — continuously monitoring control effectiveness, generating evidence packs, and surfacing drift for immediate remediation.

OUTCOME Always audit-ready, with provable, automated compliance hygiene.

5 Customisable workflows & adaptive operations

DYNAMIC WORKFLOW ENGINE · L4

Bespoke response strategies with multi-channel alerting (Slack, Teams, email, SMS), customisable SLAs and escalations, role-based segmentation, and Supply Chain Detection & Response (SCDR) for third-party risk.

OUTCOME Agile, mission-aware operations that scale and evolve with the business.

07 THE TRIQUETRA ADVANTAGE

Beyond aggregation: contextualise, orchestrate, predict.

Many platforms stop at stitching tools together. Converge360 goes further — it is the strategic intelligence layer for modern security operations.

1 Predictive defence, not reactive security

AI-SPM and dynamic risk modelling foresee threats before they materialise — shifting from reactive incident management to proactive risk mitigation.

2 True contextual awareness

LLM technology delivers clear, actionable recommendations even non-technical stakeholders understand — breaking the silos between security and the business.

3 Enterprise-ready scalability

A modular, API-first architecture integrates with both legacy infrastructure and cloud-native environments — scaling from fast-growing fintech to multinationals.

4 Trust-first design philosophy

Compliance is an operational foundation, not an afterthought — trust and transparency are embedded in every workflow, from evidence collection to continuous controls monitoring.

5 · Unified dashboard experience

Not tools stitched together — a true Singularity Dashboard. One interface. One source of truth. One step ahead.

08 CONCLUSION

Security, reimagined.

In an era of heightened cyber risk, complex IT ecosystems and strict compliance mandates, a unified security approach is no longer optional — it is essential.

Triquetra Converge360™ redefines what a modern security platform should be: **intelligent, proactive, integrative and scalable**. Whether you are combating alert fatigue, drowning in manual processes, or preparing for a regulatory audit, Converge360 provides the clarity and control needed to regain command of your security posture. It transforms **chaos into coordination, silos into synergy, and alerts into action**.

Backed by cutting-edge AI, SOAR workflows and compliance automation — and built on a five-layer architecture threaded by an agentic fabric — Converge360 doesn't just adapt to the future of cybersecurity. It defines it.

Experience security, reimagined.

Experience Triquetra Converge360™. Visit **triquetra.cc** or reach out at **info@triquetra.cc** to schedule a demo or learn more.

ABOUT TRIQUETRA

Triquetra is a purpose-built singularity platform engineered to unify visibility, intelligence and automation within a single, intelligent dashboard. It empowers security and IT teams with real-time situational awareness, AI-driven threat detection and SOAR-powered automated response. Designed for scale and enterprise complexity, Triquetra breaks down security silos, boosts operational agility, and transforms fragmented tools into a cohesive, orchestrated ecosystem — delivering continuous compliance, seamless automation and robust protection across on-premises, cloud and hybrid environments.