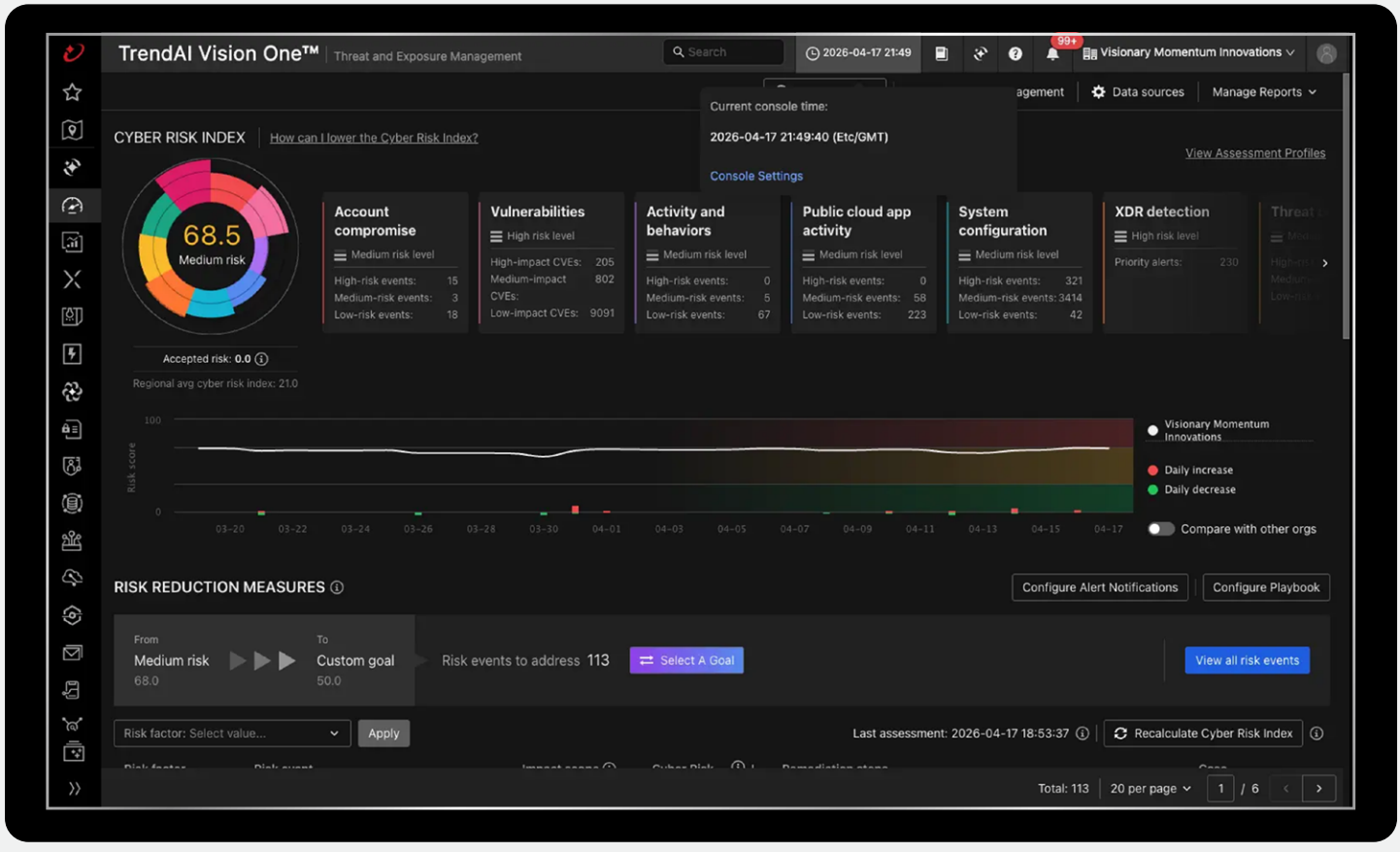
TrendAI™

Cybersecurity INSIDERS

SOLUTION REVIEW

TrendAI Vision One™

Connecting Exposure, Security Operations, and AI Security for Proactive Risk Reduction and Coordinated Response



WHY FRAGMENTED SECURITY FALLS SHORT IN THE AI ERA

Today's security architecture is the product of years of incremental expansion. Endpoint, identity, cloud, data, and now AI controls were added as new technologies and risks emerged. Each improved visibility and protection within its domain, but also introduced its own telemetry, identifiers, severity models, and workflows. And while the enterprise became more connected—security context did not.

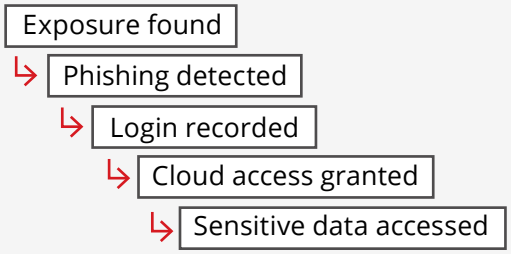
An exposure can sit in one system, the identity that can reach it in another, and the activity exploiting it in a third. Analysts must reconstruct those relationships and manually carry ownership, business importance, evidence, and response status across tools and teams. The result is missed threats, misprioritized exposures, and slower response.

68% of organizations operate seven or more cloud-security tools. Only 12% say their tools, policies, and teams work coherently. IBM's 2026 Cost of a Data Breach Report puts security complexity among the largest contributors to breach cost, now averaging $4.99 million.

AI raises the pressure further. It accelerates adversaries, adds applications, models, agents, and machine identities to secure, and makes incomplete context more consequential as more decisions become automated. What is missing is not another console or more telemetry data but a shared operating layer that connects exposure, identity, threat activity, and business impact from prioritization through investigation and response.

One attack, five disconnected signals

A cloud storage resource is flagged for overly permissive access and enters a manual remediation queue. Days later, a phishing attack compromises an employee's credentials or session. A new, unauthorized login follows; the compromised identity assumes access it is already permitted to use, and sensitive cloud data is read.



No single signal expresses the full attack. Each system can record its part correctly while missing the significance of the combined pattern. What is absent is the connection between the known exposure, the compromised identity, the activity that follows, and the business consequence of the data at risk.

THE PLATFORM RESPONSE: CONNECTING CONTEXT TO ACTION

This review examines TrendAI™ Vision One, an enterprise security platform spanning cyber risk exposure management, security operations, threat intelligence, layered protection, and AI security into a shared operating model. Specifically, it assesses how Vision One is designed to:

- **Connect asset, identity, exposure, and threat context across security domains**
- **Prioritize risk by business impact and active threat intelligence**
- **Preserve context as investigations move into response**
- **Secure AI across enterprise use, development, and runtime**

Sources: 2026 Cloud & AI Security Report, Cybersecurity Insiders | IBM Cost of a Data Breach Report 2026.

Copyright © 2026 Cybersecurity Insiders. All Rights Reserved

HOW IT WORKS:
ONE SHARED OPERATING LAYER ACROSS SECURITY DOMAINS

TrendAI Vision One brings cyber risk exposure management, security operations, and threat intelligence together across seven protection domains, including cloud, endpoint, identity, data, email, network, and AI security. Underlying Vision One is TrendAI, combining security-trained models, knowledge-graph inference, AI agents, and more than 35 years of threat intelligence to correlate assets, identities, exposures, and observed activity across one platform.

In practice, that shared foundation changes security operations in important ways:

- **Context that arrives with the alert:** Investigations begin with correlated asset, identity, vulnerability, and exposure context rather than requiring analysts to reconstruct it from scratch.
- **Prioritization tied to real adversary behavior:** TrendAI Threat Research and Intelligence, including Zero Day Initiative (ZDI) pre-disclosure insights, and sensor telemetry add exploitability and adversary context, separating theoretical exposure from risks connected to active threats.
- **Reach beyond native controls:** TrendAI's native sensors provide deep telemetry and enforcement, while TrendAI Vision One™ Agentic SIEM, APIs, and integrations extend the operating environment to third-party sources and existing security investments.
- **AI-assisted operations:** TrendAI Companion™ uses the platform's context to guide investigations, suggest next steps, generate queries, and help automate routine security work.

Together, these elements preserve rich context as risk moves from discovery to investigation and response, reducing the manual reconstruction that slows security operations.



TrendAI Vision One™ is an AI security platform that centralizes cyber risk exposure management, security operations, and layered protection.

Copyright © 2026 Cybersecurity Insiders. All Rights Reserved

FROM EXPOSURE DISCOVERY TO COORDINATED RESPONSE

Vision One's operating model starts before an incident. TrendAI™ Cyber Risk Exposure Management (CREM) identifies what is exposed, relates it to asset criticality, identity, threat activity, and business impact, and surfaces the risks that warrant attention first. When risk becomes active, that context graph carries into detection, investigation, and response rather than being rebuilt at each handoff.

STAGE	HOW VISION ONE WORKS
 **Discover, prioritize, and validate**	Maps known, unknown, unmanaged, and third-party assets, predicts and validates likely attack paths, and scores risk using asset criticality, threat activity, and business impact. The Cyber Risk Index provides a common measure for tracking posture and peer benchmarking.
 **Detect and investigate**	Correlates native and third-party telemetry with asset, vulnerability, identity, and exposure context. Workbench assembles the correlated attack, affected entities, attack paths, and threat intelligence in one investigation.
 **Mitigate and verify**	Coordinates response workflows and approvals, while native controls and integrations carry actions into containment across tools and teams. Remediation status remains visible in the wider risk view.

One attack, one connected risk story

Consider the same attack described earlier, now viewed through Vision One. CREM relates the cloud storage resource with overly permissive access to its owner, the sensitive data involved, potential attack paths, and current threat context. That allows the exposure to be prioritized by potential business impact and exploitability rather than severity alone.

If the exposure is remediated, that path to the data is closed before a compromised identity can exploit it. If it remains open, the phishing event, new login, subsequent cloud access, and sensitive-data activity are correlated with the exposure context already established. Workbench opens one investigation holding the affected identity, assets, prior exposure, attack path, and supporting evidence behind each step. Agentic SOAR coordinates the response workflows and approvals.

The operational advantage is twofold: risks with greater potential consequence can be addressed earlier, and when an incident still occurs, analysts begin with a connected risk story instead of reconstructing one from scattered evidence.



CUSTOMER OUTCOME:

Northeast Georgia Health System reports a

60%

reduction in time spent investigating false positives with TrendAI Vision One.

Copyright © 2026 Cybersecurity Insiders. All Rights Reserved

SECURING AI ACROSS USE, BUILD, AND RUN

Enterprises are putting AI into production faster than governance and security controls are keeping pace. Models serve traffic against prompts nobody anticipated. Agents hold credentials nobody scoped. Employees move company data through personal tools nobody sanctioned.

Organizations typically mature their AI security programs through four stages: Visiblity, Observability, Ownership, & Governance. TrendAI Vision One™ helps organizations advance through each stage while securing how AI is used, built, and run. The capabilities below illustrate how the platform addresses AI risk across the operational lifecycle.

AI LIFECYCLE	WHAT CAN GO WRONG	VISION ONE APPROACH
Use AI securely	An employee pastes sensitive data into an unsanctioned AI tool, or a malicious prompt slips past the enterprise boundary undetected.	Discover shadow AI, set policy controls, inspect prompts and responses for malicious activity, and block sensitive data leakage. **Vision One Capabilities: Cyber Risk Exposure Management + AI Secure Access**
Build AI securely	An AI application ships with a prompt injection flaw, a data exposure path, or an API weakness that testing missed.	Simulate attacks against the application, its models, and its APIs before deployment, then feed findings back into development. **Vision One Capabilities: AI Scanner**
Run AI securely	A running application leaks data, calls an unsafe tool, or takes an action outside its intended scope.	Apply runtime guardrails to block unsafe model outputs and actions and protect the workloads and APIs behind the application. **Vision One Capabilities: AI Guard**

An over-permissioned agent is an identity risk, a cloud risk, and a data risk at once. The work can therefore be framed in four stages: see what AI is running (visibility), catch exposures before attackers do (observability), tie every agent and tool to an owner (ownership), and prove risk is under control to the board (governance).

Vision One brings AI usage, applications, infrastructure, and agents into the broader security context already used for exposure management and security operations, helping organizations improve visibility, establish ownership, strengthen observability, and support governance across AI initiatives.

73%

of organizations are building, deploying, or operating AI applications, while only 19% govern cloud and AI together.

Copyright © 2026 Cybersecurity Insiders. All Rights Reserved

WHERE VISION ONE STANDS OUT

Vision One's differentiation is not simply the number of capabilities on the platform, but the depth behind them: a connected risk-to-response operating model, vulnerability intelligence that changes prioritization, and deployment flexibility for environments that cannot rely on SaaS alone.

1. **Connected exposure, operations, and protection:**
Vision One combines Cyber Risk Exposure Management with security operations and native controls so exposure context can influence what gets prioritized, active threat evidence can inform investigation, and response can move through the same broader operating environment. The advantage is not simply consolidation but reducing the seams between finding risk, understanding the consequences, determining whether the risk is active, and acting on it.

2. **Vulnerability intelligence with a measurable head start:**
TrendAI™ Zero Day Initiative™ (ZDI) is the world's largest vendor-agnostic vulnerability intelligence program, backed by more than 19,000 independent researchers. It's research gives customers access to exclusive pre-disclosure intelligence and access to protection up to 115 days ahead of vendor patches.

3. **Deployment choice for constrained environments:**
Vision One supports SaaS, sovereign and private cloud, and on-premises deployment, including air-gapped and offline environments. That breadth gives regulated, critical-infrastructure, and sovereignty-sensitive organizations deployment options aligned with data-residency, connectivity, and operational constraints, and extends Vision One into environments that SaaS-only architectures may not readily serve.

ENTERPRISE SCALE AND PLATFORM DURABILITY

TrendAI serves over 25,000 enterprise customers across 185 countries. Its platform credentials include four consecutive Champion placements in Omdia's Global Cybersecurity Platform Ecosystems Leadership Matrix and 21 consecutive Gartner Leader recognitions in endpoint protection.

Together, those distinctions show both current platform relevance and a long record operating across enterprise security categories.

The next question is fit: which organizations gain most from that combination of intelligence, deployment choice, and platform scale to justify broader adoption?

Copyright © 2026 Cybersecurity Insiders. All Rights Reserved

BEST FIT

Vision One is strongest when the buying decision is about connecting multiple security domains rather than replacing a single point product. Its value increases as exposure management, security operations, protection, and AI security share more context and workflows. That makes the platform particularly relevant for organizations with the following characteristics:

- **Complex enterprises** trying to connect exposure management, security operations, layered protection, and AI security across fragmented security domains and teams
- **Organizations pursuing phased platform consolidation** while retaining important third-party controls
- **Enterprises adopting AI broadly** enough to require governance across employee use, application development, runtime, and autonomous agents
- **Regulated and sovereignty-sensitive organizations** requiring private, sovereign, on-premises, air-gapped, or offline deployment options

Vision One is particularly relevant where analyst capacity is constrained or security leaders need to translate technical exposure into board-level risk and measurable posture improvement.

DEPLOYMENT AND ADOPTION

For enterprise buyers, platform fit also depends on how flexibly Vision One can be integrated into the existing environment, and expanded over time.



Deployment choice

Vision One supports SaaS, sovereign and private cloud, and on-premises deployment, including air-gapped and offline environments.



Rapid onboarding

Supported cloud capabilities can use agentless and API-based integration to establish visibility without deploying agents everywhere, with agents available where deeper runtime telemetry and protection are required.



Flexible licensing and expansion

TrendAI Flex provides a shared credit pool across 30+ Vision One solutions. Unused credits can be reassigned during the contract term as priorities change.

Copyright © 2026 Cybersecurity Insiders. All Rights Reserved

THE VERDICT: CONNECTING RISK TO ACTION

TrendAI Vision One makes a strong case for enterprise platform adoption because its capabilities reinforce one another. CREM brings business and exposure visibility and context into prioritization; XDR and Agentic SIEM connect that context to active threat evidence; Workbench carries the investigation forward; and Agentic SOAR and native controls coordinate action. AI security extends the same platform across how enterprises use, build, and run AI.

For enterprises prepared to connect security domains rather than add another isolated tool, TrendAI Vision One earns serious evaluation.

HOW TO EVALUATE VISION ONE

The most useful evaluation is not a feature checklist, but an end-to-end test of how Vision One preserves context and improves decisions as risk moves from exposure through investigation and response.

- **Establish the baseline:** Measure time from exposure discovery to prioritization and remediation, investigation time, manual handoffs, and time to containment for a representative workflow.
- **Test a cross-domain scenario:** Use a problem where fragmentation already creates friction, such as an exposed cloud resource, the identity that can reach it, and related endpoint, email, or cloud activity. Include the third-party data sources that matter in the production environment.
- **Measure context and outcome:** Confirm that asset, identity, ownership, business importance, exposure history, threat evidence, decisions, and remediation status remain connected across the workflow, then compare prioritization, investigation effort, handoffs, and response time against the baseline.

Experience TrendAI™ Vision One

WITH A FREE 30-DAY TRIAL

TrendAI™ helps enterprises predict, detect, and respond to cyber risk while enabling secure AI adoption. TrendAI Vision One is its adaptive enterprise security platform, combining cyber risk exposure management, security operations, layered protection, threat intelligence, and AI security.

TrendAI™

Copyright © 2026 Cybersecurity Insiders. All Rights Reserved