TrendAI™

Solution Brief

TrendAI Vision One™

Cyber Risk Exposure Management (CREM)

Proactively uncover, predict, assess, and mitigate cyber risks to prioritize impact, reduce exposure, and build cyber resilience

Security teams need a complete picture to effectively control risk

Not having a centralized view of risk leads to siloed data, too many alerts, not enough context, and hidden critical exposures.

Flip the script with our TrendAI Vision One™ Cyber Risk Exposure Management (CREM) solution. Prioritize visibility and give your organization the clarity needed to go from reactive to strategic. Empower your security operations with a shared understanding of where risk lives and what to do about it.

The days of reactive security are over

Security teams can't secure what they can't see. CREM addresses this head-on by delivering real-time, comprehensive visibility into your identities, devices, cloud assets, networks, applications, and more. Enable your organization to uncover unknown or unmanaged risk areas across your entire attack surface—anticipating, adapting, and acting before they become active threats. Take immediate and meaningful actions to enhance your security and compliance posture while quantifying cyber risk in business terms.

It's not just about managing threats; it's about cultivating real cyber risk resilience for your organization. Shift from reactive to proactive with CREM and TrendAI Vision One™, our industry-leading AI security platform.

A revolutionary approach

CREM empowers your cybersecurity teams to combine siloed tools and partial views for a complete picture.

Within one powerful, easy-to-use solution, merge your visibility, risk intelligence, and mitigations across cloud, data, identity, APIs, AI, compliance, and SaaS applications.

Stay ahead of adversaries and protect your business proactively with control, clarity, and confidence.

One solution, one risk picture

Complete attack surface and risk visibility

Continuous, real-time contextual insight into the entire attack surface—including known, unknown, undisclosed and third-party assets—are all mapped to business impact. By integrating compliance and cyber risk quantification, CREM delivers a complete risk picture beyond asset discovery to show true exposure.

Unmatched risk intelligence advantage

All risks are not created equal. CREM delivers the most advanced contextual risk assessments and scoring in the industry, powered by TrendAI™ Cybertron—the industry's first proactive AI for cybersecurity—the TrendAI™ Zero Day Initiative™ (ZDI), over 10 risk factors, and the broadest native sensor coverage. With 73% of global vulnerabilities in the market disclosed exclusively by TrendAI™ **according to Omdia**, customers gain exclusive pre-disclosed insights and protection 90 to 120 days before patches are available to the public. This provides a critical risk advantage.

Industry-first security and risk tool consolidation

No other solution combines as many critical security and risk disciplines into a single solution. CREM eliminates tool sprawl by replacing multiple-point solutions across external attack surface management (EASM), cloud security posture management (CSPM), vulnerability risk management (VRM), attack surface management (ASM), cyber asset attack surface management (CAASM), security awareness, and more. This reduces cost, complexity, and operational friction.

The CREM lifecycle

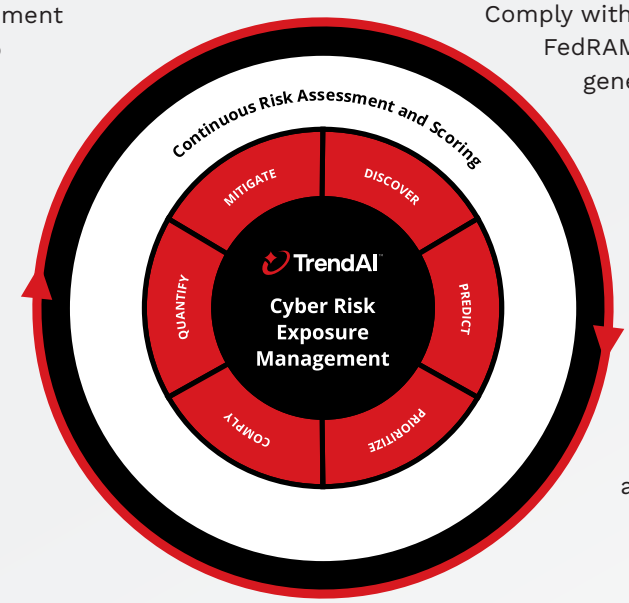
Ensure your security teams have a holistic approach to cyber risk and exposure management.

Leverage continuous risk assessment scoring for early insights to help prioritize mitigation, reduce exposure, and benchmark against peers so you stay ahead of threats.

Discover every asset across your environment using real-time discovery and risk-based vulnerability management to eliminate blind spots.

Predict attacks before they happen, using advanced threat intelligence to forecast where adversaries will strike.

Prioritize what matters the most, fast, with context-driven risk scoring that goes beyond basic severity ratings.



Comply with standards such as NIST, FedRAMP, and GDPR with instantly generated, audit-ready reports.

Quantify and clearly communicate your risk posture to stakeholders and board, driving informed, strategic decisions and investment justification.

Mitigate threats automatically using AI-guided playbooks and orchestrated remediation actions across multiple security controls.

AI Fearlessly

TrendAI Vision One™ is the only AI security platform that centralizes cyber risk exposure management, security operations, and robust layered protection to help you predict and prevent threats, accelerating proactive security outcomes.

TrendAI Vision One | Industry-Leading AI Security Platform

Cyber Risk Exposure Management
Vulnerability Management, Risk, ASM, EASM, CSPM

Security Operations
XDR, Agentic SIEM, Agentic SOAR

Threat Intelligence
Threat Intelligence Platform, Threat Intel Feed, Adversary Research

AI App Security | Cloud Security | Data Security | Email Security | Endpoint Security | Identity Security | Network Security

Services

Key capabilities	Description	Delivered by CREM
Attack surface discovery	Identify exposures across on-premises, cloud, internet-facing assets, and applications to reduce entry points for attacker.	✓
Security playbooks	Leverage automated threat response to reduce alert fatigue and accelerate remediation.	✓
Dashboards and reporting	Drill into risks and generate reports to support faster, data-driven decisions	✓
External attack surface management (EASM)	Identify and secure external-facing assets to minimize blind spots.	✓
Identity security posture	Detect identity risks using connected data sources and behavioral insights to strengthen access and control.	✓
Cloud asset inventory	Gain centralized visibility into multi-cloud environments for better cloud management.	✓
Risk assessment and prioritization	Leverage quick and frictionless risk assessments and prioritization across on-premises and cloud assets.	✓
Vulnerability risk management	Proactively identify, prioritize, and remediate high-impact vulnerabilities with speed and precision.	✓
Attack path prediction	Map how threats could spread to anticipate and block attack chains.	✓
Compliance management	Transform compliance with automated controls and actionable insights to reduce manual effort and meet compliance standards.	✓
Security awareness training	Educate users on threat behavior to reduce human error with engaging training and realistic phishing simulations.	✓
Contextual visibility and asset graphing	Visualize asset relationships to uncover hidden risks and improve response time.	✓
Container runtime vulnerability prioritization	Detect and prioritize container risks pre-runtime to block threats earlier.	✓
Cloud security posture management (CSPM)	Find cloud misconfigurations and apply best practices and frameworks to stay compliant.	✓
Agentless malware and vulnerability scanning	Continuously assess asset health to detect threats and reduce exposure.	✓
API security posture management	Detect API risks like weak authentication to secure third-party access.	✓