TrendAI™

Solution Brief

TrendAI Vision One™

Container Security

Proactive protection for every phase of your container lifecycle

Container security needs a lifecycle approach

Modern applications move fast. They're built in containers, deployed across hybrid clouds, and scaled in minutes. But speed introduces risk. Vulnerabilities, misconfigurations, and exposed secrets can slip through the cracks, especially when security is added late in the process.

TrendAI Vision One™ changes the game. It embeds protection from the very beginning—pre-runtime—and continues through runtime, giving your DevOps and SecOps teams the ability to proactively manage risk without slowing innovation.

Build phase

Image scanning

Artifact scanning

CLI GitHub integration

Deploy phase

Admission control

Image signature verification

Configuration checks

Run phase

Runtime security

Vulnerability scanning

Malware and secret scanning

KSPM compliance scanning

Figure 1: Secure containers across build, deploy, and runtime phases. Integrate with platforms like AWS, Microsoft Azure, Google Cloud , Oracle Cloud, Alibaba Cloud, Red Hat OpenShift, and self-managed Kubernetes, delivering proactive protection without disrupting DevOps workflows.

KEY BENEFITS

Proactively manage risk

Identify and address vulnerabilities, misconfigurations, and exposed secrets early in the build phase, reducing friction and downtime.

Protect without downtime

Monitor for suspicious behavior, container drift, and unauthorized access to ensure compliance and security.

Integrate seamlessly

Incorporate CI/CD pipelines and platforms like AWS, Azure, and Google Cloud into your stack for proactive protection without disrupting DevOps workflows.

Pre-runtime: Secure before you deploy

Security starts in the build phase. TrendAI Vision One™ integrates directly into CI/CD pipelines, enabling you to scan container images for vulnerabilities, malware, and secrets, before they ever reach production. Your developers can fix issues early using their existing tools, reducing friction and downtime.

Admission control policies and container image signature verification allow you to enforce compliance at deployment. Only containers that meet your security standards, such as non-privileged status or clean scan results, are allowed to run. This ensures that you can block misconfigured or risky containers before they can cause harm.

Without container security, your applications are exposed to vulnerabilities and misconfigurations, opening the door for attackers to exploit.

Runtime: Continuous protection in production

Once containers are running, TrendAI Vision One™ provides you with deep visibility and protection. Leverage our runtime security scan to monitor for suspicious behavior, container drift, and unauthorized access. Kubernetes Security Posture Management (KSPM) enables you to ensure ongoing compliance with Center for Internet Security (CIS), National Security Agency (NSA), and other benchmarks.

Extended detection and response (XDR) telemetry allows you to correlate container activity with broader threat intelligence, enabling faster investigation and response. Whether you're running on AWS, Azure, Google Cloud, or on-premises, runtime protection adapts to your environment.

Find and fix vulnerabilities, malware, and misconfigurations before they become a problem.

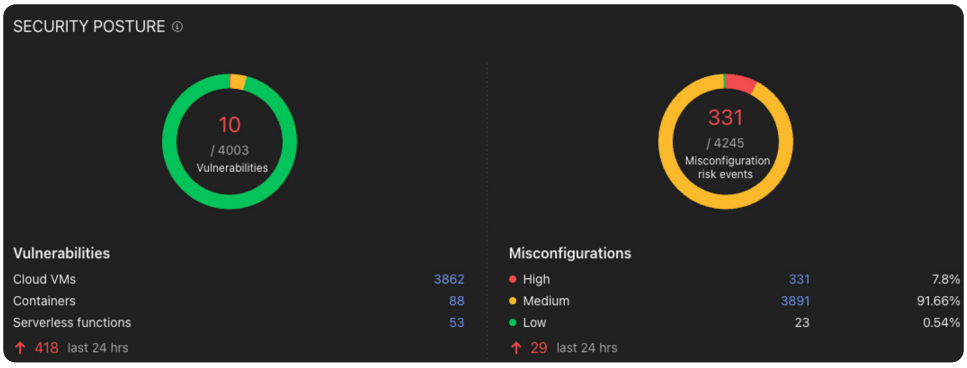


Figure 2: Real-time view of container security, showing alerts, compliance status, and workload risk at a glance.

From reactive cleanup to proactive risk management

Go beyond detection: predict. Attack path analysis lets you identify how threats could move through your environment, highlighting crown jewel assets at risk. Agentless scanning enables you to ensure zero impact on workloads while uncovering vulnerabilities, malware, and exposed secrets, so you can add layers of protection for containerized services and help your team stay ahead of attackers.

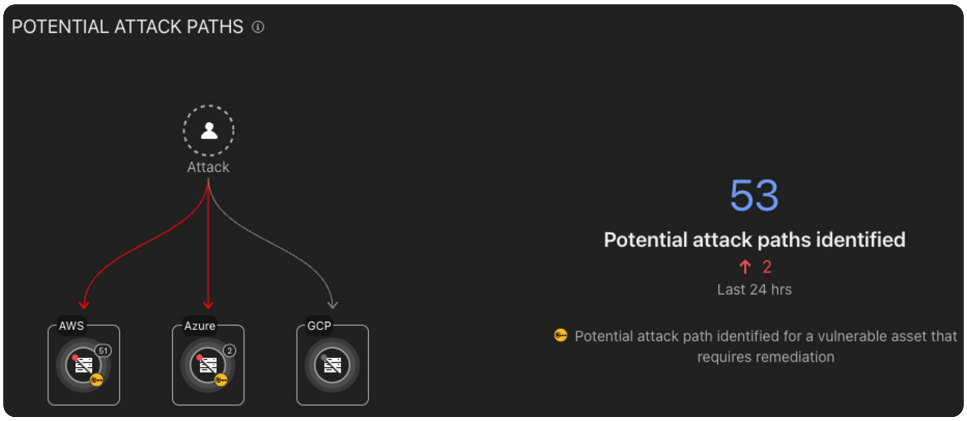
Securing the AI infrastructure powering your business

Most mainstream AI training and inference workloads are widely deployed in containers, and a large number of AI services run on containerized environments. Container security is therefore a critical layer of your overall AI security strategy, spanning the computing layer, model layer, data layer, pipeline layer, network layer, and application layer.

This creates new and distinct risk dimensions that sit on top of what traditional container security already addresses. Model weights can be exfiltrated through compromised containers. Training data can be poisoned via misconfigured pipelines, while inference endpoints, often internet-exposed by design, become entry points for adversaries. TrendAI Vision One™ adds dedicated AI-specific protection on top of traditional container security capabilities, giving your teams visibility into the risks that matter most for AI workloads.

Leverage agentless scanning to uncover exposed secrets and vulnerabilities in model serving containers without impacting performance. Runtime monitoring continuously watches for abnormal behaviors inside running containers, so you can catch threats that static scanning alone would miss.

As organizations navigate an evolving AI regulatory landscape, including frameworks like the NIST AI Risk Management Framework and the EU AI Act, TrendAI Vision One™ helps your teams build a defensible, auditable approach to AI infrastructure security.



Unified visibility and contextual insights

Your security teams need more than alerts; they need context. TrendAI Vision One™ offers you a project view of container risks, so you can align security with business priorities. Group risks by application or business unit and enrich them with telemetry and cloud tags.

Organize cloud risk by what matters most: your projects.

Platform coverage that meets you where you are

Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Service (ECS), AWS Fargate

Azure Kubernetes Service (AKS)

Google Kubernetes Engine (GKE)

Oracle Cloud

Alibaba Cloud Container Service for Kubernetes (ACK)

Red Hat OpenShift

TrendAI™: A recognized leader in cloud-native security

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

IDC

Named a Leader in IDC MarketScape: Worldwide Cloud-Native Application Protection Platform 2025 Vendor Assessment

Gartner

Recognized as a 2024 Gartner® Peer Insights™ Customers' Choice for Cloud-Native Application Protection Platforms

MITRE

Achieved 100% detection of major attack steps in MITRE Engenuity™ ATT&CK Evaluations

Gartner

Named a Leader in the 2025 Gartner® Magic Quadrant for Endpoint Protection Platforms for the 20th time

System requirements

- Kubernetes 1.14+ (certified)
- Helm 3.0.1+
- Compatible with major cloud providers and on-premises environments

See it in action

See firsthand how our AI-powered enterprise cybersecurity platform proactively protects your most valuable assets and accelerates business growth.

Try TrendAI Vision One™ for free

Visit trendmicro.com/trials